afi
120 Belmont Drive
Somerset, NJ 08873-1204
american fibertek
Phone: 732.302.0660 Fax: 732.302.0667

SM10p-PoE

8 (10/100TX) + 2 Gigabit Copper/SFP Combo with 8 PoE Injectors Managed Switch

SM10p-PoE

Instruction Manual

2012-09

Regulatory Approval
- FCC Class A
- UL 1950
- CSA C22.2 No. 950
- EN60950
- CE
- EN55022 Class A
- EN55024

Canadian EMI Notice

This Class A digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

European Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community Compliance with these directives imply conformity to the following European Norms:

EN55022 (CISPR 22) - Radio Frequency Interference
EN61000-X - Electromagnetic Immunity
EN60950 (IEC950) - Product Safety

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Contents

FCC Warning i
CE Mark Warning.....ii

Introduction 1

Features..... 2
Software Feature 4
Package Contents..... 7

Hardware Description 8

Physical Dimension..... .8
Front Panel 8
LED Indicators 10
Rear Panel..... ..12
Desktop Installation..... ..13
Attaching Rubber Pads 13
Power On..... .13

Network Application 14

Small Workgroup 15
Segment Bridge 16

Console Management 18

Login in the Console Interface.....18
CLI Management 19
Commands Level 20
Commands Set List 22
System Commands Set.....22
Port Commands Set 25

Trunk Commands Set 27
VLAN Commands Set 29
Spanning Tree Commands Set 31
QOS Commands Set.....33
IGMP Commands Set 34
Mac / Filter Table Commands Set 34
SNMP Commands Set 35
Port Mirroring Commands Set 38
802.1x Commands Set.....38
TFTP Commands Set.....41
SystemLog, SMTP and Event Commands Set.....42
SNTP Commands Set 43
X-ring Commands Set 45

Web-Based Management 46

About Web-based Management..... 46
Preparing for Web Management..... 46
System Login 46
System Information 47
IP Configuration 48
DHCP Configuration 49
DHCP Server Configuration 50
DHCP Client Entries.....51
Port and IP Bindings.....51
TFTP - Update Firmware 52
TFTP - Restore Configuration 53
TFTP - Backup Configuration..... 53
System Event Log Configuration..... 54
System Event Log - SMTP Configuration 55
System Event Log - Event Configuration.....56

SNTP Configuration 58
IP Security 61
User Authentication..... 62
Port Statistics 63
Port Control..... 64
Port Trunk 65
Port Trunk - Aggregator setting 65
Port Trunk - Aggregator Information.....66
Port Trunk - State Activity.....67
Port Mirroring 68
Rate Limiting..... 69
VLAN configuration 70
VLAN configuration - Port-based VLAN 71
802.1Q VLAN 74
802.1Q Configuration.....75
Group Configuration 76
Rapid Spanning Tree 77
RSTP - System Configuration 77
RSTP - Port Configuration.....79
SNMP Configuration 80
System Configuration 80
Trap Configuration.....82
SNMPV3 Configuration 82
QoS Configuration 86
QoS Policy and Priority Type 86
Port Base Priority 88
COS Configuration 88
TOS Configuration.....88
IGMP Configuration 88
X-Ring..... 91

802.1X/Radius Configuration 93
System Configuration 93
802.1x Per Port Configuration 94
Misc Configuration 95
MAC Address Table 96
Static MAC Address.....96
MAC Filtering 97
All MAC Addresses.....98
Power over Ethernet 100
Factory Default..... 101
Save Configuration 102
System Reboot 102
Troubleshooting.....103
Incorrect connections 103
- ❐ Faulty or loose cables.....103
- ❐ Non-standard cables 103
- ❐ Improper Network Topologies.....104

Diagnosing LED Indicators..... 104
Technical Specification 105
Appendix.....108
Console Port Pin Assignments..... 108
100BASE-TX/10BASE-T Pin Assignments 109
RJ-45 Pin Assignment of non-802.3af standard PD with Midspan/Endspan POE HUB/SWITCH 109

Introduction

Power-over-Ethernet (PoE) eliminates the need to run power to other devices on a wired LAN. Using Power-over-Ethernet systems installers needs to run only a single Category 5 Ethernet cable that carries both power and data to each device. This allows for greater flexibility in the location of network devices and significantly decreasing installation costs in many cases.

There are two system components in PoE—the Power Sourcing Equipment (PSE) initiates the connection to the second component, and the Powered Device (PD). The current is transmitted over two of the four twisted pairs of wires in a Category-5 cable.

Power over Ethernet follows the IEEE 802.3af and is completely compatible with existing Ethernet switches and networked devices. Because the Power Sourcing Equipment (PSE) tests whether a networked device is PoE-capable, power is never transmitted unless a Powered Device is at other end of the cable. It also continues to monitor the channel. If the Powered Device does not draw a minimum current, because it has been unplugged or physically turned off, the PSE shuts down the power to that port. Optionally, the standard permits Powered Devices to signal to the PSEs exactly how much power they need.

The 8 10/100TX + 2 Gigabit copper/Mini-GBIC Combo with 8 PoE Injectors Managed Switch and the 8 10/100TX + 1 10/100/1000T/100/1000 SFP Combo with 4 PoE Injectors Managed Switch are the multi-port switches that can be used to build high-performance switched workgroup networks. Both switches are a store-and-forward device that offers low latency for high-speed networking. It also features a “store-and-forward “switching scheme. This allows the switch to auto-learn and store source address in an 8K-entry MAC address table. The switch is targeted at workgroup, department or backbone computing environment.

Features

System Interface/Performance

- RJ-45 ports support Auto MDI/MDI-X Function
- Embedded 4-port or 8-port PoE injector function
- Store-and-Forward Switching Architecture
- Back-plane (Switching Fabric): 5.6Gbps (8 10/100TX + 2 Giga Copper/Mini-GBIC Combo model)
- Back-plane (Switching Fabric): 3.6Gbps (8 10/100TX + 1 10/100/1000T/100/1000 SFP Combo model)
- 1Mbits Packet Buffer
- 8K MAC Address Table

VLAN

- Port Based VLAN
- Support 802.1 Q Tag VLAN
- GVRP
- Double Tag VLAN (Q in Q)*

Port Trunk with LACP

8 10/100TX + 2 Giga Copper/Mini-GBIC Combo model supports 802.1ab LLDP**

QoS (Quality of Service)

- Support IEEE 802.1p Class of Service
- Per port provides 4 priority queues
- Port Base, Tag Base and Type of Service Priority

Port Mirror: Monitor traffic in switched networks.

- TX Packet only
- RX Packet only
- Both of TX and RX Packet

Security

- Port Security : MAC address entries/filter
- IP Security : IP address security management to prevent unauthorized intruder.
- Login Security: IEEE802.1X/RADIUS

IGMP with Query mode for Multi Media Application

Spanning Tree

- Support IEEE802.1d Spanning Tree
- Support IEEE802.1w Rapid Spanning Tree

X-ring

- X-ring, Dual Homing, and Couple Ring Topology
- Provide redundant backup feature and the recovery time below 300ms

Support 802.1ab LLDP **

Bandwidth Control

- Ingress Packet Filter and Egress Rate Limit
- Broadcast/Multicast Packet Filter Control

System Event Log

- System Log Server/Client
- SMTP e-mail Alert

SNMP Trap

- Device cold start
- Authentication failure
- X-ring topology changed
- Port Link up/Link down
- PoE Status *

TFTP Firmware Update and System Configure Restore and Backup

* Future Release

** Optional

Software Feature

Management	SNMP v1 SNMP v2c SNMP v3 Web/Telnet/Console (CLI)/Menu Driven**
VLAN	Port based VLAN IEEE802.1Q Tag VLAN(256 entries) / VLAN ID(Up to 4K, VLAN ID can be assigned from 1 to 4094) GVRP (256 Groups) Double Tag VLAN (Q in Q)*
Port Trunk with LACP	LACP Port Trunk: 4 trunk groups of maximum 4 trunk members
LLDP**	Supports LLDP that allows switch to advertise its identification and capability on the LAN
Spanning Tree	IEEE802.1d Spanning tree IEEE802.1w Rapid spanning tree
X-ring	Supports X-ring, Dual Homing, and Couple Ring Provides redundant backup feature and recovery time below 300ms
Quality of service	The quality of service determined by port, Tag and IPv4 Type of service, IPv4/IPv6 Different Service
Class of Service	Supports IEEE 802.1p Class of Service, per port provides 4 priority queues Weight Round Ratio (WRR)‰ High: Mid-High: Mid-Low: Low (8:4:2:1)

Port Security	Supports100 entries of MAC address for static MAC and another 100 for MAC filter
Port Mirror	Supports 3 mirroring types: “RX, TX and Both packet”
IGMP	Supports IGMP snooping v1 and v2 256 multicast groups IGMP query mode
IP Security	Supports 10 IP addresses that have permission to access the switch management to prevent unauthorized intruder
Bandwidth Control	Supports ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 100Kbps (10/100) and 256Mbps (1000) Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet, Broadcast/Multicast packet, Broadcast only and all of packet The packet filter rate can be set as 100Kbps (10/100) and 256Mbps (1000)
User Authentication	Supports IEEE802.1x User Authentication and can report to RADIUS server
Flow Control	Supports Flow Control for Full-duplex and Back Pressure for Half-duplex

System log	Supports System log record and remote system log server
SMTP	Supports SMTP Server and 6 email accounts for receiving event alert
SNMP Trap	Up to 3 Trap stations Cold start, Port link down, Port link up, authorization failure, PoE status, X-ring topology change
DHCP	DHCP Client DHCP Server
DNS	Provides DNS client feature and supports Primary and Secondary DNS server
SNTP	Supports Simple Network Time Protocol to synchronize system clock in Internet
Firmware Upgrade	Supports TFTP firmware upgrade
Configuration Upload and Download	Supports binary format configuration file for system quick installation (TFTP backup and restore)

* Future Release

** Optional

Package Contents

Unpack the contents of the 8 10/100TX + 2 Gigabit copper/Mini-GBIC Combo with 8 PoE Injectors Managed Switch. Verify against the checklist below:

- (1) 8 10/100TX + 2 Gigabit copper/Mini-GBIC Combo with 8 PoE Injectors Managed Switch
- (4) Rubber Pads
- (1) RS-232 cable
- (1) Power Cord
- (1) User Manual

8 10/100TX plus 2 Gigabit copper/MINI-GBIC Combo with 8 PoE Injectors Managed

Rubber Pads

RS-232 cable

Power Cord

User Manual

Compare the contents of the package with the standard checklist above. If any item is missing or damaged, please contact the local dealer for exchanging.

Hardware Description

This section mainly describes the hardware of the PoE Injector Managed Switch and gives a physical and functional overview on the certain switch.

Physical Dimension

SM10p-PoE 8 10/100TX + 2 Gigabit copper/Mini-GBIC Combo with 8 PoE Injectors Managed Switch's physical dimensions is 270mm(W) x 210mm(D) x 44mm(H).

Front Panel

The front panel of the 8 10/100TX + 2 Gigabit copper/Mini-GBIC Combo with 8 PoE Injectors Managed Switch consists of 8 x 10/100Base-TX RJ-45 Ethernet ports (Auto MDI/MDIX), 2 Giga port and 2 Mini-GBIC ports. The LED Indicators are also located on the front panel of the switch.

The Front panel of the 8 10/100TX + 2 Gigabit copper/Mini-GBIC Combo with 8 PoE Injectors Managed Switch

- RJ-45 Ports: 8 x 10/100 N-way auto-sensing for 10Base-T or 100Base-TX connections. Moreover, these ports also supply power for PDs.

  In general, MDI means connecting to another Hub or Switch while MDIX means connecting to a workstation or PC. Therefore, Auto MDI/MDIX would allow connecting to another switch or workstation without changing non-crossover or crossover cabling.
- 2 Gigabit Ethernet port: 2 x 10/100/1000TX N-Way auto-sensing for 10/100/1000 connection.
- 2 Mini-GBIC port: 2 mini-GBIC ports for Gigabit or 100M fiber connection.

LED Indicators

The LED Indicators display real-time information of systematic operation status. The following table provides descriptions of LED status and their meaning.

The LED indicators description of 8 10/100TX + 2 Gigabit Copper/Mini-GBIC Combo model

	Status	Description
LED	Green	Power On
Power	OFF	No power inputs
	Green	The port is supplying power to the connected powered-device
FWD (port 1~8)	OFF	No powered device attached or power supplying failed
	Green	The port is operating at speed of 1000M
1000M (RJ45 port 9~10)	OFF	The port is disconnected or not operating at speed of 1000M
	Green	Connected to network
LK/ACT (port 1~ 10)	Blinking	Networking is active
	OFF	Not connected to network
	Green	The port is operating at speed of 100M
100M	OFF	The port is disconnected or not operating at speed of 100M

LK/ACT (MINI GBIC 9, 10)	Green	Connected to network
	Blinking	Networking is active
	OFF	Not connected to network

Rear Panel

The 3-pronged power plug and terminal block are located on the rear panel of the 8 10/100TX + 2 Gigabit copper/Mini-GBIC Combo with 8 PoE Injectors Managed Switch as shown below. The switch will work with AC in the voltage range of AC 100-240V with Frequency of 50-60Hz, or work with DC 48V which is the redundant power supply for the switch.

The Rear Panel of the 8 10/100TX + 2 Gigabit copper/ MINI GBIC Combo with 8 PoE Injector Managed Switch

Desktop Installation

Set the switch on a sufficiently large flat space with a power outlet nearby. The surface where you put the switch should be clean, smooth, level and sturdy. Make sure there is enough clearance around the switch to allow attachment of cables, power cord and allow air circulation.

Attaching Rubber Pads

A. Make sure mounting surface on the bottom of the switch is grease and dust free.
B. Remove adhesive backing from your Rubber Pads.
C. Apply the Rubber Pads to each corner on the bottom of the switch. These footpads can prevent the switch from shock/vibration.

Power On

Connect the power cord to the power socket on the rear panel of the switch. The other side of power cord connects to the power outlet. The internal power supply of the switch works with voltage range of AC in the 100-240VAC/ Frequency of 50~60Hz, or the redundant power of DC 48V for 8 10/100TX + 2 Gigabit copper/Mini-GBIC Combo with 8 PoE Injectors Managed Switch. Check the power indicator on the front panel to see if power is properly supplied.

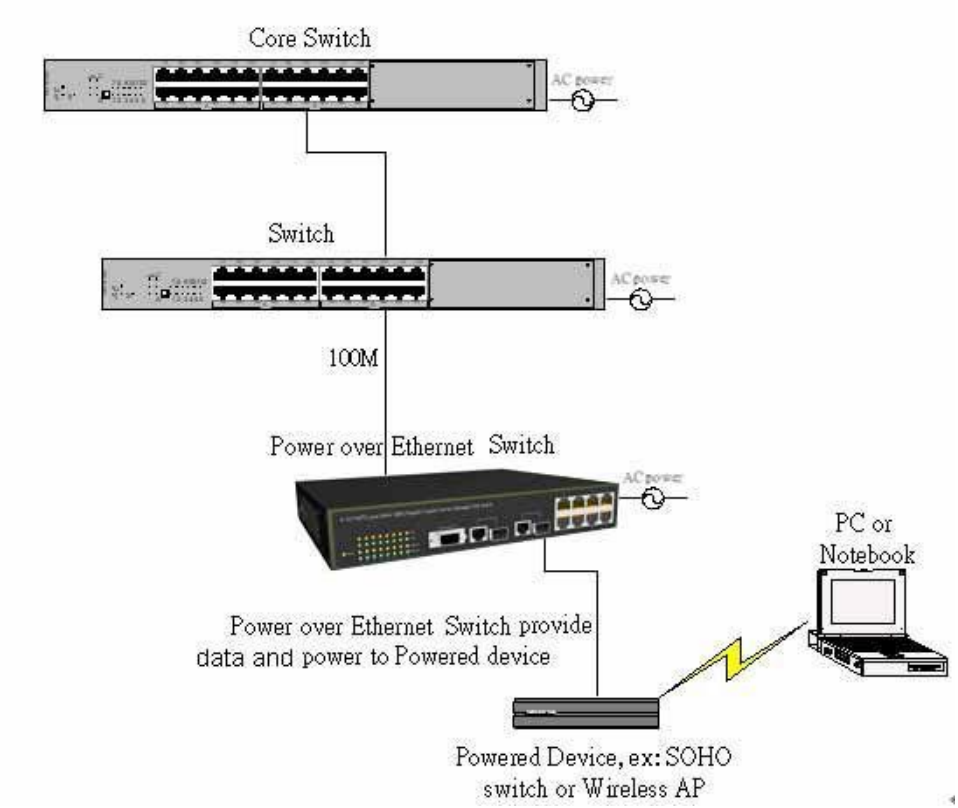
Network Application

This section provides a few samples of network topology in which the switch is used. In general, the PoE Injector Managed Switch is designed as a segment switch which has large address table (8k MAC addresses) and high performance to deal with interconnecting networking segments.

PC, workstations, and servers can communicate each other by directly connecting with PoE injector Managed Switch. The switch automatically learns nodes addresses, which are subsequently used to filter and forward all traffic based on the destination address.

Using the uplink port (Giga Combo port), the switch can connect with another switch or hub to interconnect other small-switched workgroups to form a larger switched network. Meanwhile, user can also use fiber ports to connect switches. The PoE switch also injects power into the UTP cables for supplying the power that PDs (Power Devices) need.

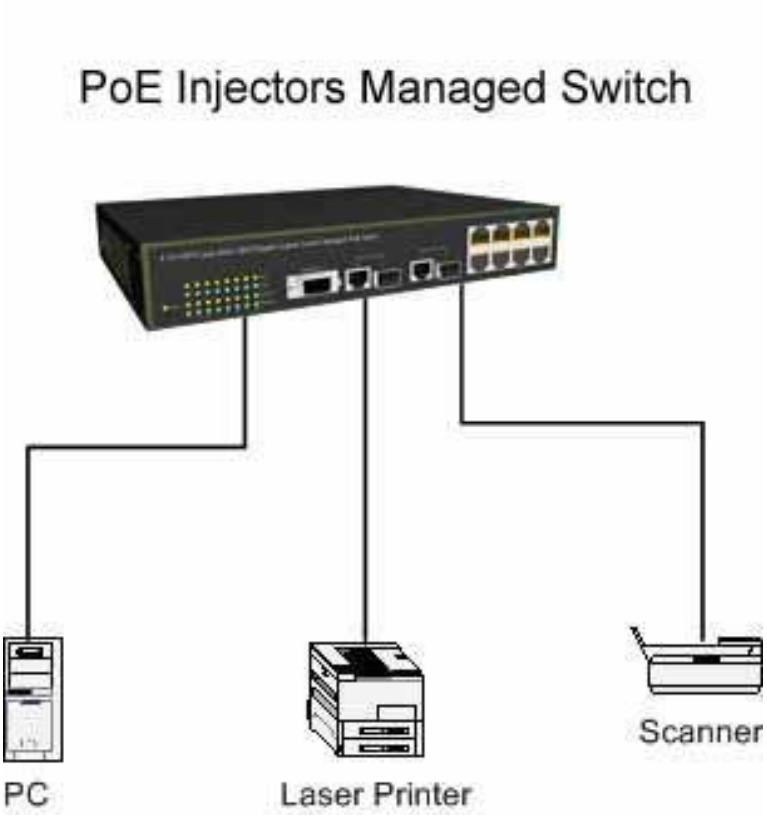
The Power over Ethernet Switch can provide power to PDs that follow the IEEE 802.3af standard in the network. It can solve the problem of position limitation. The network devices can be installed in more appropriate position for better performance. The following figure is an example of network application for Power over Ethernet Switch.



Power over Ethernet Switch network application

Small Workgroup

The PoE Injector Managed Switch can be used as a standalone switch to which personal computers, server, printer server, are directly connected to form a small workgroup.

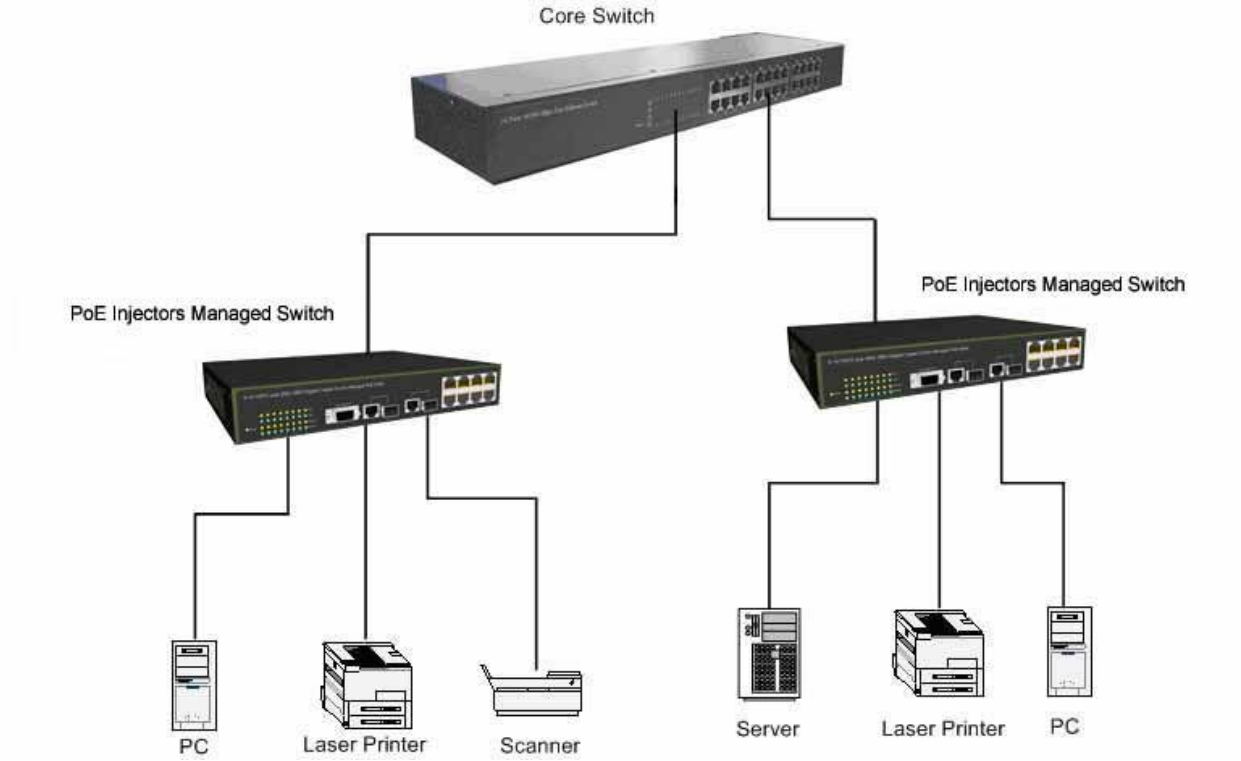


Small Workgroup application

Segment Bridge

For enterprise networks where large data broadcasts are constantly processed, this switch is an ideal solution for department users to connect to the corporate backbone.

In the illustration below, two Ethernet switches with PCs, print server, and local server attached, are both connected to the switch. All the devices in this network can communicate with each other through the switch. Connecting servers to the switch allows other users to access the data on server.



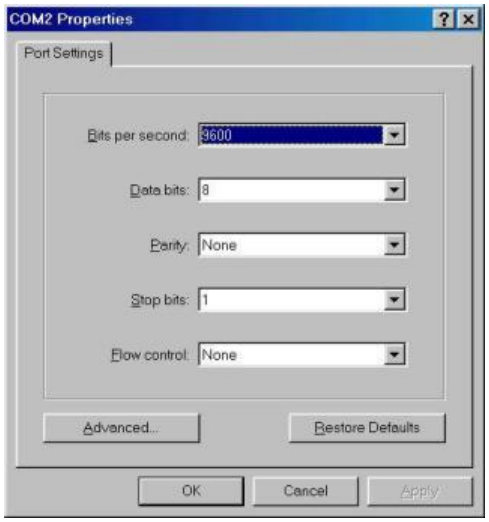
Segment Bridge application

Console Management

Login in the Console Interface

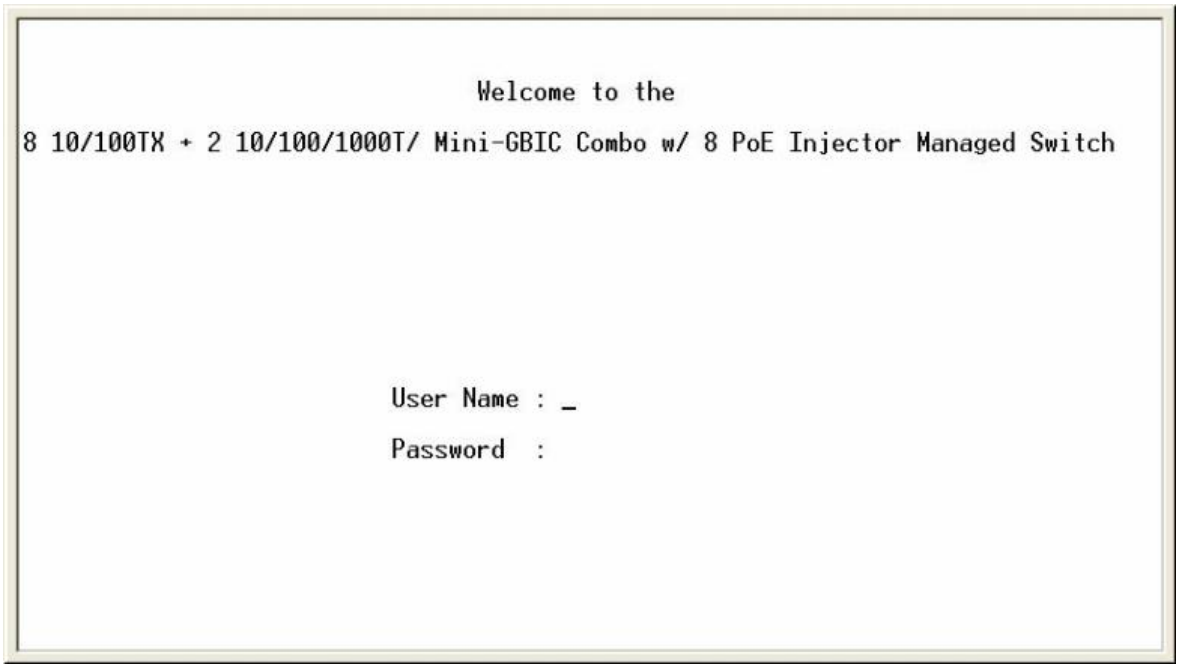
When the connection between switch and PC is ready, turn on the PC and run a terminal emulation program or Hyper Terminal and configure its communication parameters to match the following default characteristics of the console port:

Baud Rate: 9600 bps
Data Bits: 8
Parity: none
Stop Bit: 1
Flow control: None



The settings of communication parameters

After finishing the parameter settings, click "OK". When the blank screen shows up, press Enter key to bring out the login prompt. Key in the 'root' (default value) for both User name and Password (use Enter key to toggle), then hit Enter key and the console management appears right after. Please see the figure below for login screen.



Console login screen

CLI Management

The system supports console management – CLI command. After you login to the system, you will see a command prompt. To enter CLI management interface, enter "enable" command. The following table lists the CLI commands and description.

CLI command interface

Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode1
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in user	switch#	Enter disable to exit.	The privileged command is in advanced mode Privileged this mode

	EXEC mode.			to • Display advanced function status • Save configuration
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface) while in global configuration mode	switch (config-if)#	To exit to global configuration mode, enter exit. To exist to privileged EXEC mode, or end.	Use this mode to configure parameters for the switch and Ethernet ports.

Commands Set List

User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

System Commands Set

Commands	Level	Description	Example
show config	E	Show switch configuration	switch>show config
show terminal	P	Show console information	switch#show terminal
write memory	P	Save user configuration into permanent memory (flash rom)	switch#write memory
system name [System Name]	G	Configure system name	switch(config)#system name xxx
system location [System Location]	G	Set switch system location string	switch(config)#system location xxx
system description [System Description]	G	Set switch system description string	switch(config)#system description xxx
system contact [System Contact]	G	Set switch system contact window string	switch(config)#system contact xxx
show system-info	E	Show system information	switch>show system-info
ip address [Ip-address] [Subnet-mask]	G	Configure the IP address of switch	switch(config)#ip address 192.168.16.1 255.255.255.0 192.168.16.254

[Gateway]			
ip dhcp	G	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	P	Show IP information of switch	switch#show ip
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	G	Halt and perform a cold restart	switch(config)#reload
default	G	Restore to default	switch(config)#default
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)#admin username xxxxxx
admin password [Password]	G	Specifies a password (maximum 10 words)	switch(config)#admin password xxxxxx
show admin	P	Show administrator information	switch#show admin
dhcpserver enable	G	Enable DHCP Server	switch(config)#dhcpserver enable
Dhcpserver disable	G	Disable DHCP Server	switch(config)#no dhcpserver
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)#dhcpserver lowip 192.168.1.100
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)#dhcpserver highip 192.168.1.200
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	G	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	G	Configure DNS IP for DHCP clients	switch(config)#dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [Hours]	G	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding	I	Set static IP for DHCP	switch(config)#interface

[IP address]		clients by port	fastEthernet 2 switch(config)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	P	Show client entries of DHCP server	switch#show dhcpserver clients
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server function	switch(config)#no dhcpserver
security enable	G	Enable IP security function	switch(config)#security enable
security http	G	Enable IP security of HTTP server	switch(config)#security http
security telnet	G	Enable IP security of telnet server	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)#security ip 1 192.168.1.55
show security	P	Show the information of IP security	switch#show security
no security	G	Disable IP security function	switch(config)#no security
no security http	G	Disable IP security of HTTP server	switch(config)#no security http
no security telnet	G	Disable IP security of telnet server	switch(config)#no security telnet

Port Commands Set

Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to 'accept all frame'	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all

bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to 'accept broadcast, multicast, and flooded unicast frame'	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to 'accept broadcast and multicast frame'	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to 'only accept broadcast frame'	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100
bandwidth out [Value]		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
show bandwidth	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth

state [Enable | Disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

Trunk Commands Set

Commands	Level	Description	Example
aggregator priority [1~65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Group ID] [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group	G	Assign a trunk group	switch(config)#aggregator group

[GroupID] [Port-list] lacp workp [Workport]		with LACP active. [GroupID] :1~4 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
aggregator group [GroupID] [Port-list] nolacp	G	Assign a static trunk group. [GroupID] :1~4 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggregator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch#show aggregator 1 or switch#show aggregator 2 or switch#show aggregator 3
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggreator group 2

VLAN Commands Set

Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#vlan database
Vlanmode [portbase| 802.1q | gvrp]	V	To set switch VLAN mode.	switch(vlan)#vlanmode portbase or switch(vlan)#vlanmode 802.1q or switch(vlan)#vlanmode gvrp
no vlan	V	No VLAN	Switch(vlan)#no vlan
Ported based VLAN configuration			
vlan port-based grpname [Group Name] grpid [GroupID] port [PortNumbers]	V	Add new port based VALN	switch(vlan)#vlan port-based grpname test grpid 2 port 2-4 or switch(vlan)#vlan port-based grpname test grpid 2 port 2,3,4
show vlan [GroupID] or show vlan	V	Show VLAN information	switch(vlan)#show vlan 23
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#no vlan group 2
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] vid [VID]	V	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#vlan 8021q name test vid 22
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by port, if the	switch(vlan)#vlan 8021q port 3 access-link untag 33

		port belong to a trunk group, this command can't be applied.	
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)#vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q trunk [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 access-link untag 33
vlan 8021q trunk [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q trunk 3 trunk-link tag 3-20
vlan 8021q trunk [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8
show vlan [GroupID] or show vlan	V	Show VLAN information	switch(vlan)#show vlan 23
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#no vlan group 2

Spanning Tree Commands Set

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)#spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree	G	Use the spanning-tree	switch(config)#spanning-tree

forward-time [seconds]		forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	forward-time 20
stp-path-cost [1~200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-priority 128

		a port priority that is used when two switches tie for position as the root switch.	
stp-admin-p2p [Auto|True|False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-p2p Auto
stp-admin-edge [True|False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-edge True
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-non-stp False
show spanning-tree	E	Displays a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

QOS Commands Set

Commands	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low

qos priority cos [Priority][lowest|low|middle|high]	G	Configure COS Priority	switch(config)#qos priority cos 0 middle
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Displays the information of QoS configuration	Switch#show qos
no qos	G	Disable QoS function	switch(config)#no qos

IGMP Commands Set

Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
Igmp-query auto	G	Set IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	G	Set IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#show igmp multi
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	G	Disable IGMP query	switch#no igmp-query

Mac / Filter Table Commands Set

Commands	Level	Description	Example
mac-address-table static	I	Configure MAC	switch(config)#interface

hwaddr [MAC]		address table of interface (static).	fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Show all MAC address table	switch#show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

SNMP Commands Set

Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#snmp system-name l2switch
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#snmp system-location lab
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#snmp system-contact where

snmp agent-mode [v1v2c|v3|v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2cv3
snmp community-strings [Community] right [RO/RW]	G	Add SNMP community string.	switch(config)#snmp community-strings public right rw
snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.1.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.1.50
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#snmpv3 context-name Test
snmpv3 user [User Name] group [Group Name] password [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmpv3 user test01 group G1 password AuthPW PrivPW
snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv]	G	Configure the access table of SNMPV3 agent	switch(config)#snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1

match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]			
snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]	G	Configure the mibview table of SNMPV3 agent	switch(config)#snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1
show snmp	P	Show SNMP configuration	switch#show snmp
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.1.50
no snmpv3 user [User Name]	G	Remove specified user of SNMPv3 agent.	switch(config)#no snmpv3 user Test
no snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views	G	Remove specified access table of SNMPv3 agent.	switch(config)#no snmpv3 access context-name Test group G1 security-level AuthPr iv match-rule Exact views V1 V1 V1

[Read View Name] [Write View Name] [Notify View Name]			
no snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]	G	Remove specified mibview table of SNMPV3 agent.	switch(config)#no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1

Port Mirroring Commands Set

Commands	Level	Description	Example
monitor rx	G	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	G	Set TX destination port of monitor function	switch(config)#monitor tx
show monitor	P	Show port monitor information	switch#show monitor
monitor [RX|TX|Both]	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	I	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	I	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

802.1x Commands Set

Commands	Level	Description	Example

8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiusip [IP address]	G	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radius server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1

8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate	I	Use the 802.1x port	switch(config)#interface

[disable | reject | accept | authorize]		state interface configuration command to set the state of the selected port.	fastethernet 3 switch(config-if)#8021x portstate accept
show 8021x	E	Displays a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	G	Disable 802.1x function	switch(config)#no 8021x

TFTP Commands Set

Commands	Level	Description	Defaults Example
backup flash:backup_cfg	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
systemlog ip [IP address]	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode [client|server|both]	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Displays system log.	Switch>show systemlog
show systemlog	P	Show system log client & server information	switch#show systemlog
no systemlog	G	Disable systemlog functon	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)#smtp account User
smtp password [password]	G	Configure authentication password	switch(config)#smtp password
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	P	Show the information of SMTP	switch#show smtp
no smtp	G	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	G	Set cold start event type	switch(config)#event device-cold-start both
event authentication-failure [Systemlog|SMTP|Both]	G	Set Authentication failure event type	switch(config)#event authentication-failure both

event X-ring-topology-change [Systemlog|SMTP|Both]	G	Set X-ring topology changed event type	switch(config)#event X-ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	I	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	I	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	P	Show event selection	switch#show event
no event device-cold-start	G	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	G	Disable Authentication failure event typ	switch(config)#no event authentication-failure
no event X-ring-topology-change	G	Disable X-ring topology changed event type	switch(config)#no event X-ring-topology-change
no event systemlog	I	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	I	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp
show systemlog	P	Show system log client & server information	switch#show systemlog

SNTP Commands Set

Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable

sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set timezone index, use 'show sntp timzezone' command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
show sntp timezone	P	Show index number of time zone list	switch#show sntp timezone
no sntp	G	Disable SNTP function	switch(config)#no sntp

no sntp daylight	G	Disable daylight saving time	switch(config)#no sntp daylight

X-ring Commands Set

Commands	Level	Description	Example
Xring enable	G	Enable X-ring	switch(config)#Xring enable
Xring master	G	Enable ring master	switch(config)#Xring master
Xring couplering	G	Enable couple ring	switch(config)#Xring couplering
Xring dualhoming	G	Enable dual homing	switch(config)#Xring dualhoming
Xring ringport [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)#Xring ringport 7 8
Xring couplingport [Coupling Port]	G	Configure Coupling Port	switch(config)#Xring couplingport 1
Xring controlport [Control Port]	G	Configure Control Port	switch(config)#Xring controlport 2
Xring homingport [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)#Xring homingport 3
show Xring	P	Show the information of X - Ring	switch#show Xring
no Xring	G	Disable X-ring	switch(config)#no X ring
no Xring master	G	Disable ring master	switch(config)# no Xring master
no Xring couplering	G	Disable couple ring	switch(config)# no Xring couplering
no Xring dualhoming	G	Disable dual homing	switch(config)# no Xring dualhoming

Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

On the CPU board of the switch there is an embedded HTML web site residing in flash memory, which offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft
Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0. And, it is applied with Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

Preparing for Web Management

Before using web management, user can use console to login the switch to check the default IP of the switch. Please refer to Console Management Chapter for console login.
If user needs to change IP address for the first time, user can use console mode to
modify it. The default value is as below:

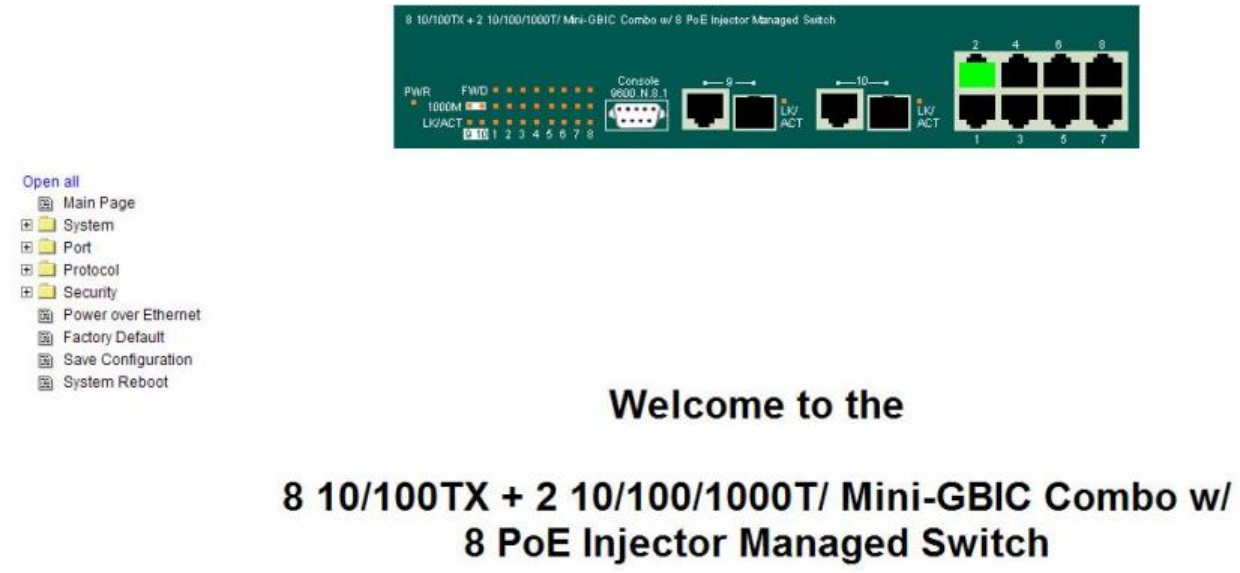
IP Address: 192.168.1.77
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.254
User Name: root Password: root

System Login

¢ Launch the Internet Explorer.

- Key in “http://” + “IP Address” of the Switch, and then press “Enter”
- Login screen will appear right after
- Key in the user name and password. The default user name and password is “root”
- Click “Enter” or” OK”, then the home screen of the Web-based management appears right after

Note: The web interface features shown below are introduced by the screen displays of 8 10/100 TX + 2 10/100/1000T/Mini-GBIC Combo (SM10P-POE) model. Unless specifically identified, the all of the screen displays are suitable for the models in this manual.



Main interface

System Information

Assign the system name and location and view the system information

- System Name: Assign the system name of the switch (The maximum length is 64 bytes)

- System Location: Assign the switch physical location (The maximum length is 64 bytes)
- System Description: Displays the description of switch(Read only cannot be modified)
- Firmware Version: Displays the switch's firmware version
- Kernel Version: Displays the kernel software version
- MAC Address: Displays the unique hardware address assigned by manufacturer (default)
- And than, click Apply

System Information interface

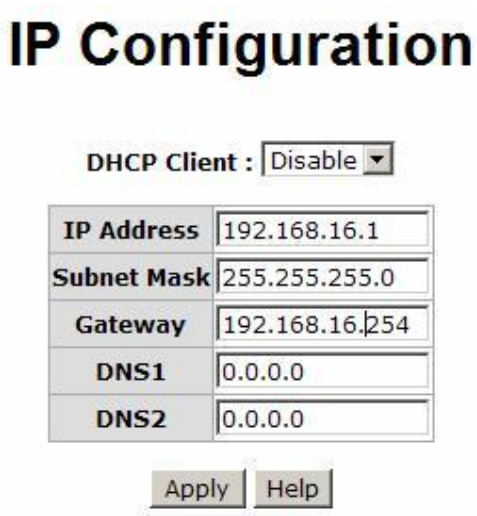
IP Configuration

User can configure the IP Settings and DHCP client function

- DHCP: Disable or enable the DHCP client function
- IP Address: Assign the switch IP address. The default IP is 192.168.1.77
- Subnet Mask: Assign the switch IP subnet mask
- Gateway: Assign the switch gateway. The default value is 192.168.1.254
- DNS1: The abbreviation of Domain Name Server—an Internet service that translates domain name into IP addresses. Domain name are alphabetic which

are easy to be remembered. Because the Internet is based on IP address; every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.net.com might translate to 192.168.1.1

- DNS2: The backup for DNS1. When DNS1 cannot function, DNS2 will then replace DNS1 immediately
- And than, click Apply
- Save after assigning the IP address



IP Configuration interface

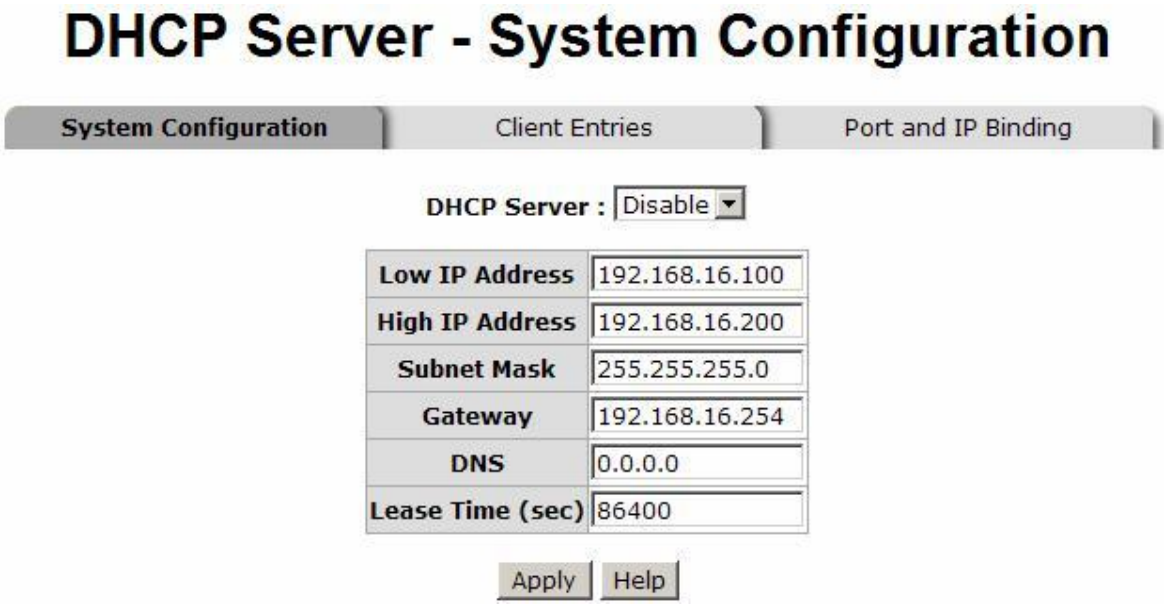
DHCP Configuration

DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Server Configuration

The system provides the DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

- DHCP Server: Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network
- Low IP Address: The dynamic IP range. Low IP address is the beginning of the dynamic IP range. For example: dynamic IP range is from 192.168.1.100 ~ 192.168.1.200. In contrast, 192.168.1.100 is the Low IP address
- High IP Address: The dynamic IP range. High IP address is the end of the dynamic IP range. For example: dynamic IP range is from 192.168.1.100 ~ 192.168.1.200. In comparison, 192.168.1.200 is the High IP address
- Subnet Mask: The dynamic IP assign range subnet mask
- Gateway: The gateway in your network
- DNS: The IP Address of the Domain Name Server in your network
- Lease Time (sec): It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle



DHCP Server Configuration interface

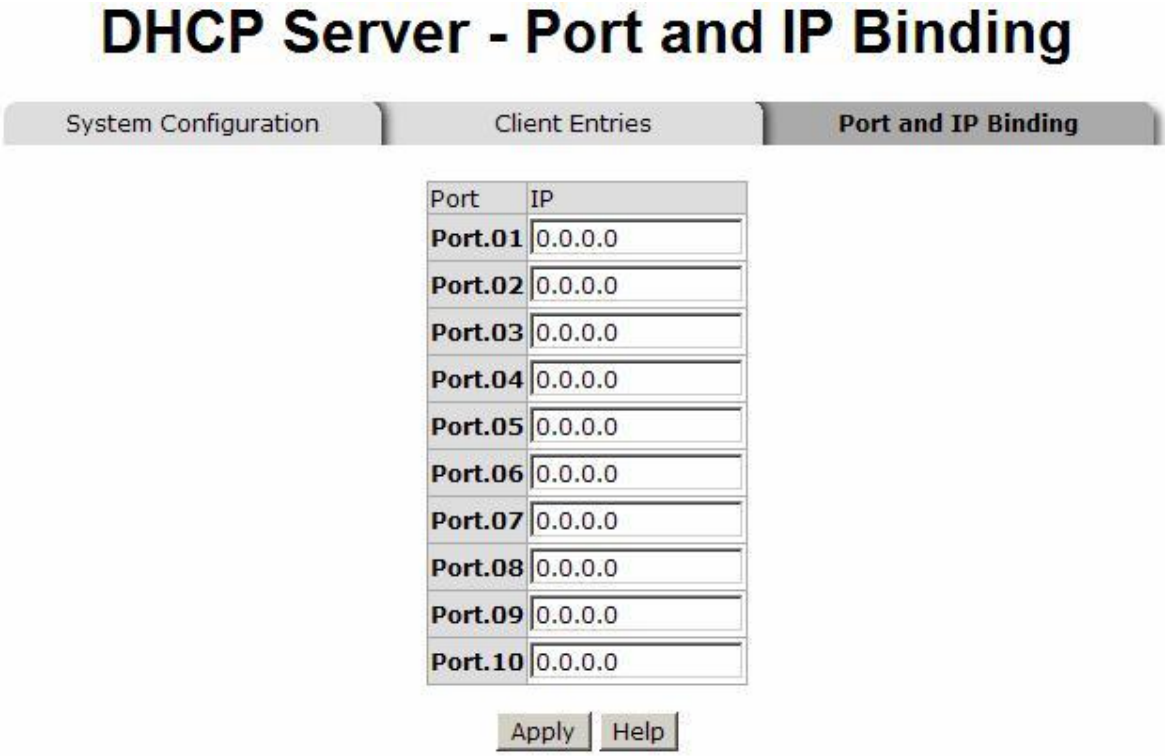
DHCP Client Entries

When the DHCP server function is active, the system will collect the DHCP client information and display it here.

DHCP Client Entries interface

Port and IP Bindings

Assign the dynamic IP address to the port. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address that has been assigned before to the connected device.



Port and IP Bindings interface

TFTP - Update Firmware

It provides the functions that allow user to update the switch firmware. Before updating, make sure the TFTP server is ready and the firmware image is on the TFTP server.

- ¢ TFTP Server IP Address: Key in the TFTP server IP
- ¢ Firmware File Name: The name of firmware image
- ¢ And then, click Apply

Update Firmware interface

TFTP - Restore Configuration

Restore EEPROM value from TFTP server

- ¢ TFTP Server IP Address: Key in the TFTP server IP
- ¢ Restore File Name: Key in the restore file image name
- ¢ And then, click Apply

Restore Configuration interface

TFTP - Backup Configuration

Save current EEPROM value from the switch to TFTP server, then go to the TFTP

restore configuration page to restore the EEPROM value.

- ¢ TFTP Server IP Address: Key in the TFTP server IP
- ¢ Backup File Name: Key in the file image name
- ¢ And then, click Apply

Backup Configuration interface

System Event Log Configuration

Configure the system event mode, which you want to collect, and system log server IP.

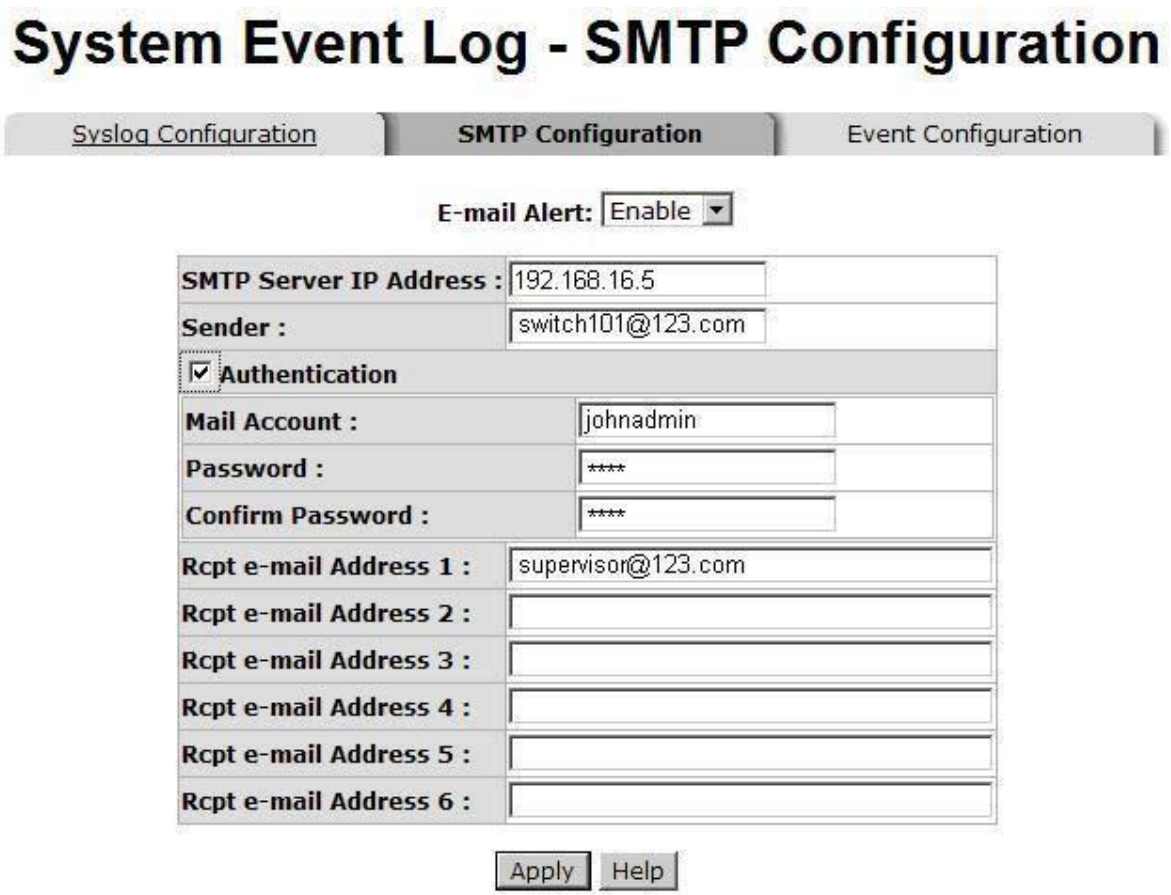
- ¢ System Log Client Mode: Select the system log mode – client only, server only, or both S/C
- ¢ System Log Server IP Address: Assign the system log server IP
- ¢ Click Reload to refresh the events log
- ¢ Click Clear to clear all current events log

System Log Configuration interface

System Event Log - SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.

- Email Alert: enable or disable the email alert function.
- SMTP Server IP: set up the mail server IP address (when Email Alert enabled, this function will then be available).
- Sender: key in a complete email address, e.g. switch101@123.com, to identify where the event log comes from.
- Authentication: mark the check box to enable and configure the email account and password for authentication (when Email Alert enabled, this function will then be available).
- Mail Account: set up the email account, e.g. johnadmin, to receive the alert. It must be an existing email account on the mail server, which you had set up in SMTP Server IP Address column.
- Password: The email account password.
- Confirm Password: reconfirm the password.
- Rcpt e-mail Address 1 ~ 6: you can assign up to 6 e-mail accounts also to receive the alert.
- Click Apply .



SMTP Configuration interface

System Event Log - Event Configuration

Select the system log and SMTP events. When selected events occur, the system will result the log information. Also, per port log and SMTP events can be selected.

¢ System event selection: 4 selections – Device cold start, Device warm start, SNMP Authentication Failure, and X - ring topology change. Mark the checkbox to select the event. When selected events occur, the system will produce the logs

‹ Device cold start: When the device executes cold start action, the system will produce a log event

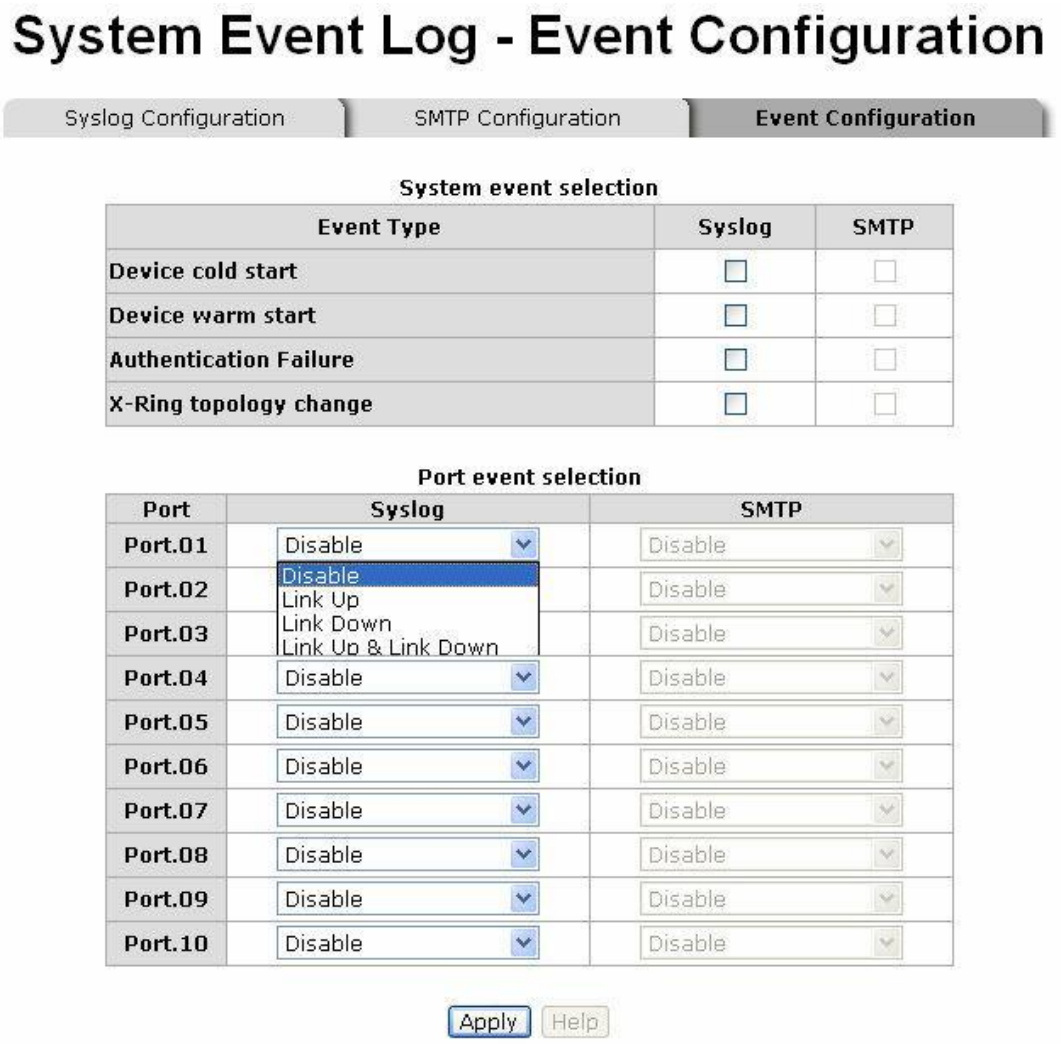
‹ Device warm start: When the device executes warm start, the system will produce a log event

‹ Authentication Failure: When the SNMP authentication fails, the system will

produce a log event

‹ X-Ring topology change: When the X-ring topology has changed, the system will produce a log event

¢ And then, click Apply



Event Configuration interface

¢ Port event selection: Select the per port events and per port SMTP events. It has 3 selections – Link UP, Link Down, and Link UP & Link Down. Disable means no event is selected

‹ Link UP: The system will result a log message when port connection is up only

‹ Link Down: The system will result a log message when port connection is down only

‹ Link UP & Link Down: The system will result a log message when port connection is up and down

SNTP Configuration

You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

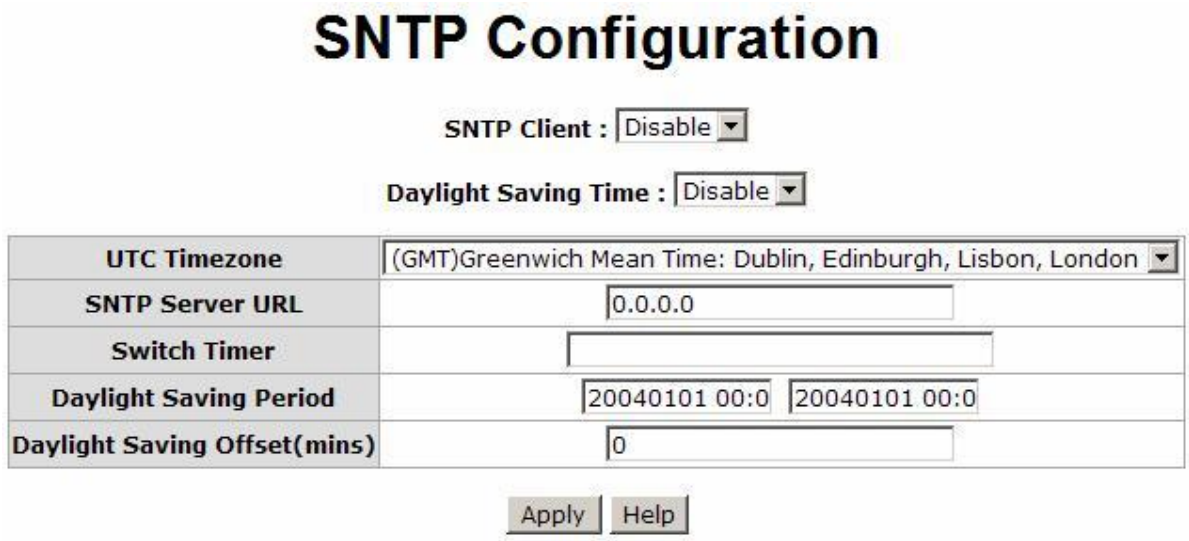
1. SNTP Client: enable or disable SNTP function to get the time from the SNTP server.
2. Daylight Saving Time: enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period.
3. UTC Timezone: set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard	-7 hours	5 am

PDT - Pacific Daylight		
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian	+10 hours	10 pm

Standard GST Guam Standard, USSR Zone 9		
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

4. SNTP Sever URL: set the SNTP server IP address.
5. Daylight Saving Period: set up the Daylight Saving beginning time and Daylight
   Saving ending time. Both will be different in every year.
6. Daylight Saving Offset (mins): set up the offset time.
7. Switch Timer: Displays the switch current time.
8. Click Apply .



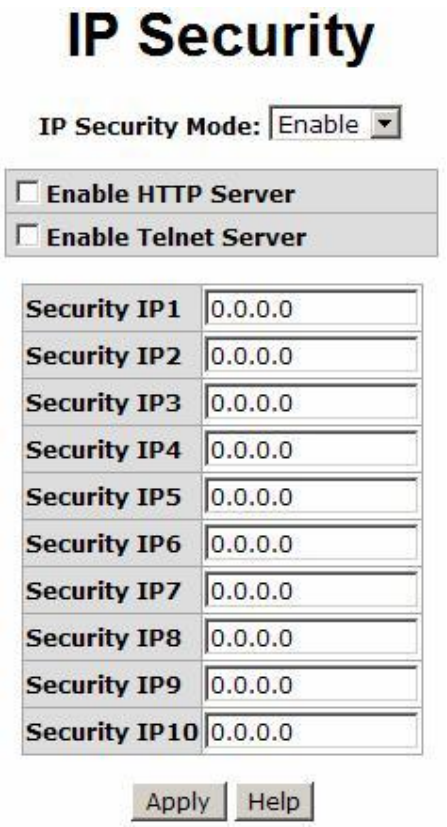
SNTP Configuration interface

IP Security

IP security function allows user to assign 10 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

- IP Security Mode: when this option is in Enable mode, the Enable HTTP Server and Enable Telnet Server check boxes will then be available.
- Enable HTTP Server: when this check box is checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via HTTP service.
- Enable Telnet Server: when checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via telnet service.
- Security IP 1 ~ 10: Assign up to 10 specific IP address. Only these 10 IP address can access and manage the switch through the Web browser
- And then, click Apply button to apply the configuration

Note Remember to execute the 'Save Configuration' action, otherwise the new configuration will lose when switch power off.



IP Security interface

User Authentication

You can change login user name and password for the management security issue

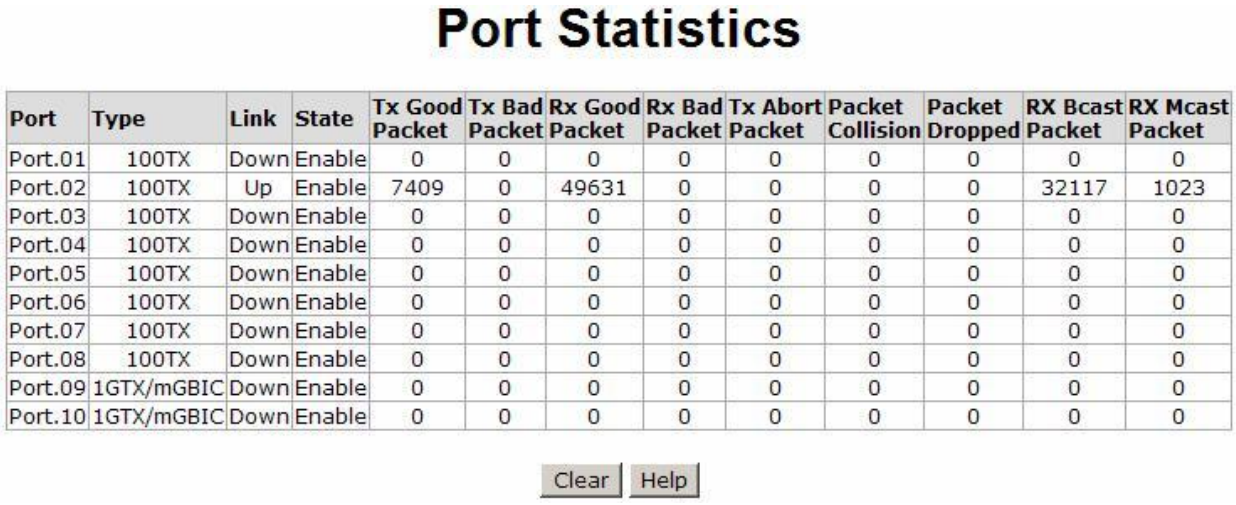
1. User name: Key in the new user name (The default is 'root')
2. Password: Key in the new password (The default is 'root')
3. Confirm password: Re-type the new password
4. And then, click Apply

User Authentication interface

Port Statistics

The following information provides the current port statistic information.

- ¢ Port: The port number.
- ¢ Type: Displays the current speed of connection to the port.
- ¢ Link: The status of linking—'Up' or 'Down'.
- ¢ State: It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
- ¢ Tx Good Packet: The counts of transmitting good packets via this port.
- ¢ Tx Bad Packet: The counts of transmitting bad packets (including undersize [less than 64 bytes], oversize, CRC Align errors, fragments and jabbers packets) via this port.
- ¢ Rx Good Packet: The counts of receiving good packets via this port.
- ¢ Rx Bad Packet: The counts of receiving bad packets (including undersize [less than 64 bytes], oversize, CRC error, fragments and jabbers) via this port.
- ¢ Tx Abort Packet: The aborted packet while transmitting.
- ¢ Packet Collision: The counts of collision packet.
- ¢ Packet Dropped: The counts of dropped packet.
- ¢ Rx Bcast Packet: The counts of broadcast packet.
- ¢ Rx Mcast Packet: The counts of multicast packet.
- ¢ Click Clear button to clean all counts.

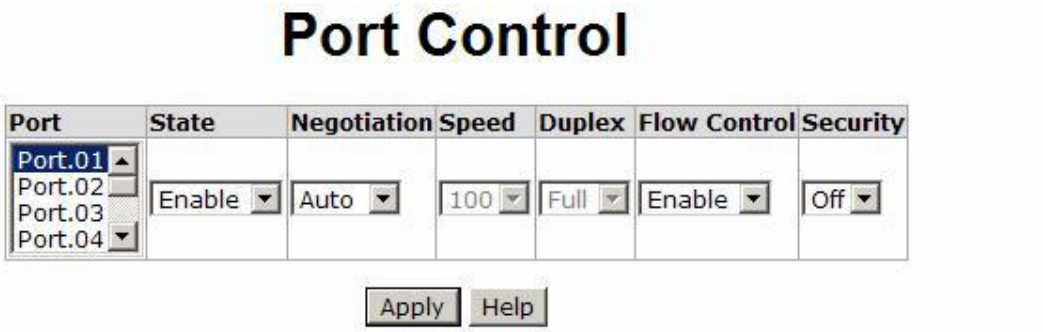

Port Statistics
Port Type Link State Tx Good Packet Tx Bad Packet Rx Good Packet Rx Bad Packet Tx Abort Packet Packet Collision Packet Dropped RX Bcast Packet RX Mcast Packet
Port.01 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.02 100TX Up Enable 7409 0 49631 0 0 0 0 32117 1023
Port.03 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.04 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.05 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.06 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.07 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.08 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.09 1GTX/mGBIC Down Enable 0 0 0 0 0 0 0 0 0
Port.10 1GTX/mGBIC Down Enable 0 0 0 0 0 0 0 0 0
Clear
Help

Port Statistics interface

Port Control

In Port control, you can view every port status that depends on user setting and the negotiation result.

1. Port: select the port that you want to configure.
2. State: Current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.
3. Negotiation: set auto negotiation status of port.
4. Speed: set the port link speed.
5. Duplex: set full-duplex or half-duplex mode of the port.
6. Flow Control: set flow control function as Enable or Disable in Full Duplex mode. The default value is Enable.
7. Security: When its state is 'On' that means this port accepts only one MAC address which was configured to be a static MAC address.
8. Click Apply.



Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.02	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Enable	ON	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.09	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
Port.10	N/A	1GTX/mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Port Control interface

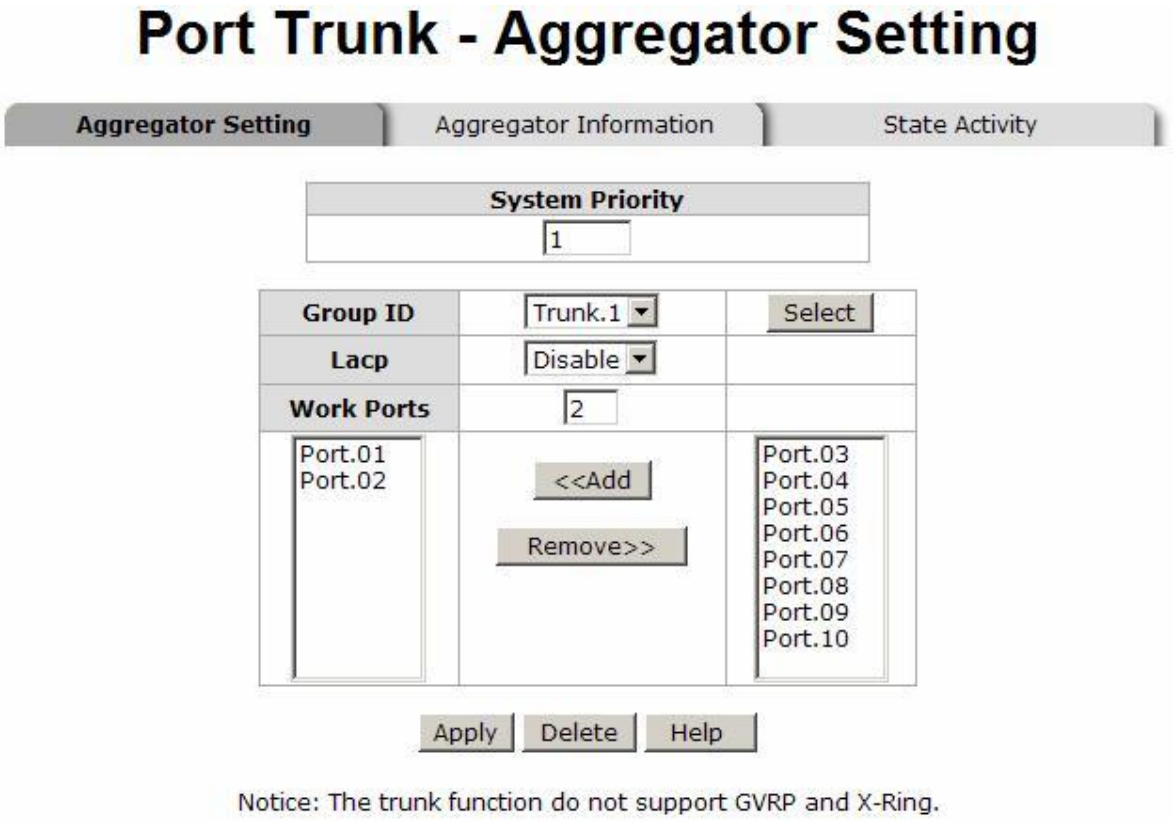
Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to 4 ports into one dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode, for more detail information please refer to IEEE 802.3ad.

Port Trunk - Aggregator setting

1. System Priority: A value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.
2. Group ID: There are four trunk groups to provide configuration. Choose the "Group ID" and click Select.
3. LACP: If enable, the group is LACP static trunk group. If disable, the group is local static trunk group. All ports support LACP dynamic trunk group. While connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.
4. Work ports: Allow up to four ports to be aggregated at the same time. With LACP static trunk group, the exceed ports are standby and can be aggregated later if work ports fail. If it is local static trunk group, the number of ports must be the same as the group member ports.
5. Select the ports to join the trunk group. Click Add button to add the port. To remove unwanted ports, select the port and click Remove button.
6. If LACP enable, you can configure LACP Active/Passive status in each ports on State Activity page.
7. Click Apply.

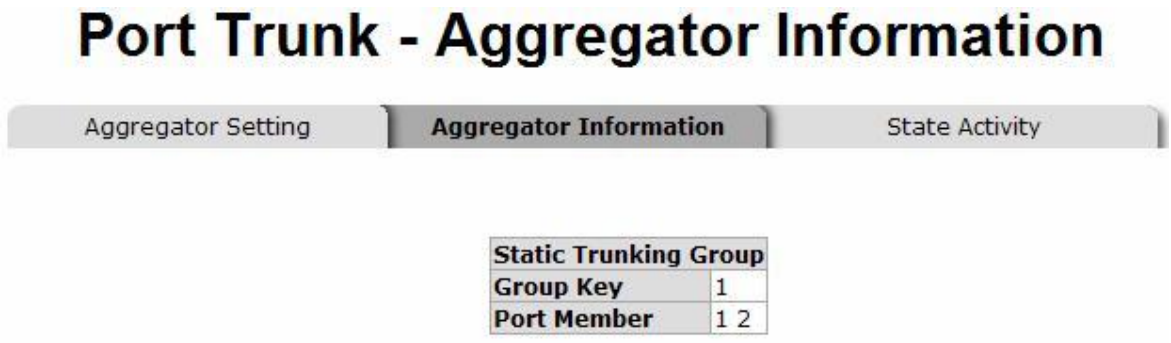
8. Use Delete button to delete Trunk Group. Select the Group ID and click Delete button.



Port Trunk—Aggregator Setting interface

Port Trunk - Aggregator Information

When you have setup the aggregator setting with LACP disabled, you will see the local static trunk group information here.



Port Trunk – Aggregator Information interface

Port Trunk - State Activity

When you had setup the LACP aggregator, you can configure port state activity. You can mark or un-mark the port. When you mark the port and click Apply button the port state activity will change to Active. Opposite is Passive.

- ¢ Active: The port automatically sends LACP protocol packets.
- ¢ Passive: The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

Note 1. A link has either two active LACP ports or one active port can perform dynamic LACP trunk.

2. A link has two passive LACP ports will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.
3. If you are active LACP's actor, after you have selected trunk port, the active status will be created automatically.

Port Trunk – State Activity interface

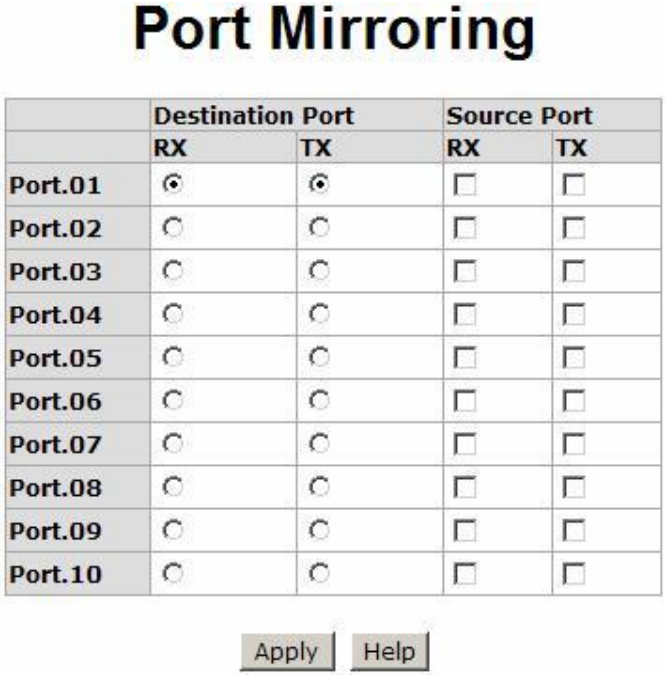
Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored via one specific port. That means traffic goes in or out monitored (source) ports will be duplicated into mirror (destination) port.

¢ Destination Port: You can select one port to be the destination (mirror) port for monitoring both RX and TX traffic which come from source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. User can connect mirror port to LAN analyzer or Netxray

¢ Source Port: The ports that user wants to monitor. All monitored port traffic will be copied to mirror (destination) port. User can select multiple source ports by checking the RX or TX check boxes to be monitored.

¢ And then, click Apply button.



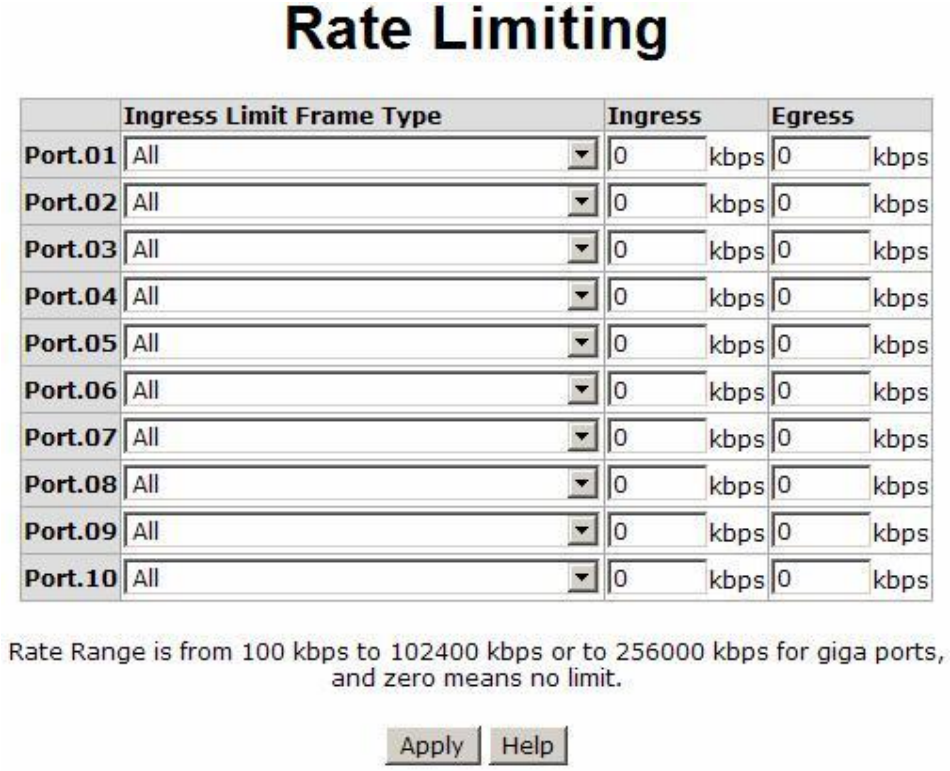
Port Trunk – Port Mirroring interface

Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

¢ Ingress Limit Frame type: Select the frame type you want to filter. The frame types have 4 options for selecting: All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and Broadcast only.

Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and Bbroadcast only types are only for ingress frames. The egress rate only supports All type.


Rate Limiting
Ingress Limit Frame Type
Ingress
Egress
Port.01 All 0 kbps 0 kbps
Port.02 All 0 kbps 0 kbps
Port.03 All 0 kbps 0 kbps
Port.04 All 0 kbps 0 kbps
Port.05 All 0 kbps 0 kbps
Port.06 All 0 kbps 0 kbps
Port.07 All 0 kbps 0 kbps
Port.08 All 0 kbps 0 kbps
Port.09 All 0 kbps 0 kbps
Port.10 All 0 kbps 0 kbps
Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.
Apply
Help

Rate Limiting interface

¢ All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate as 1Mbps, ingress rate as 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate

‹ Ingress: Enter the port effective ingress rate (The default value is '0')

‹ Egress: Enter the port effective egress rate (The default value is '0')

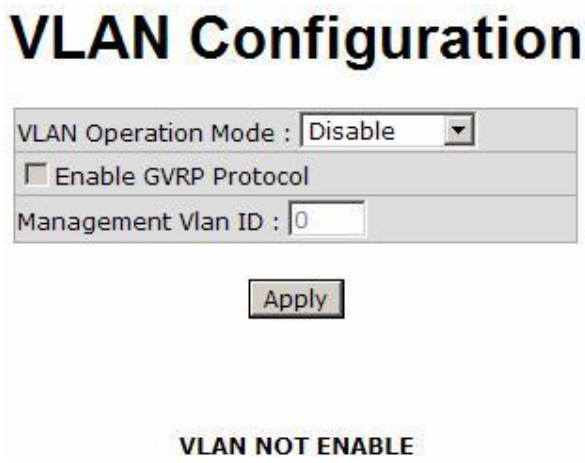
¢ And then, click Apply to apply the settings

VLAN configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which would allow you to isolate network traffic, so only the members of the same VLAN will receive traffic from each other. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch.

However, all the network devices are still plugged into the same switch physically.

The switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is ‘Disable’.

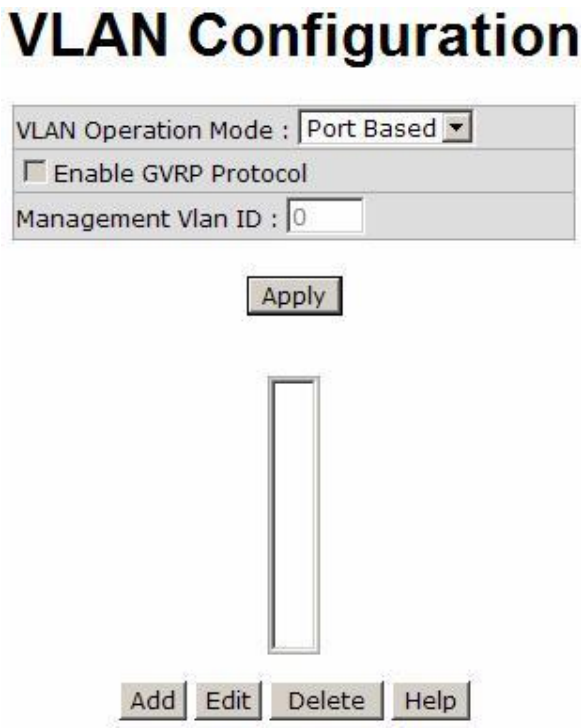


VLAN Configuration interface

VLAN configuration - Port-based VLAN

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored.

In order for an end station to send packets to different VLAN groups, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

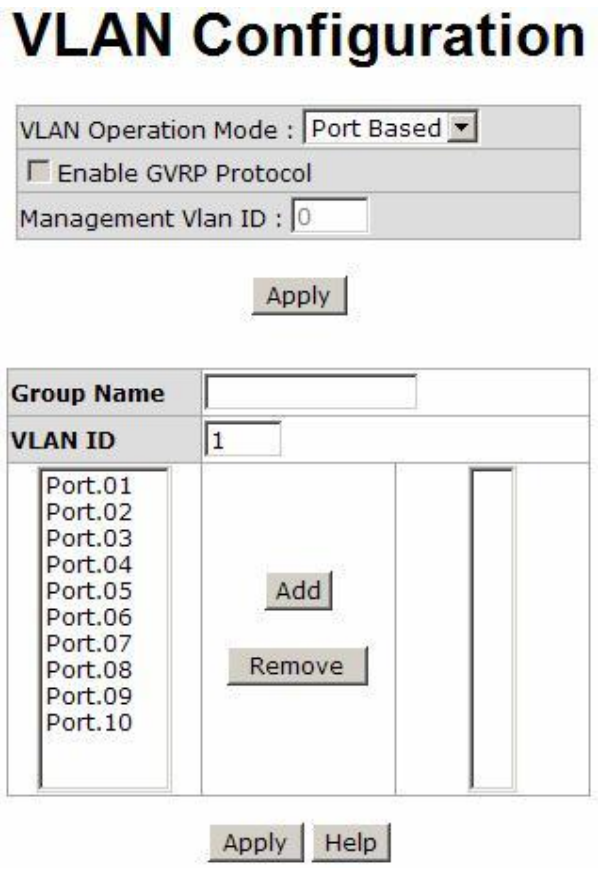


VLAN – Port Based interface

¢ Click Add to add a new VLAN group (The maximum VLAN group is up to 256 VLAN groups)

¢ Entering the VLAN name, group ID and grouping the members of VLAN group

¢ And then, click Apply



VLAN—Port Based Add interface

¢ You will see the VLAN displays.

¢ Use Delete button to delete unwanted VLAN.

¢ Use Edit button to modify existing VLAN group.

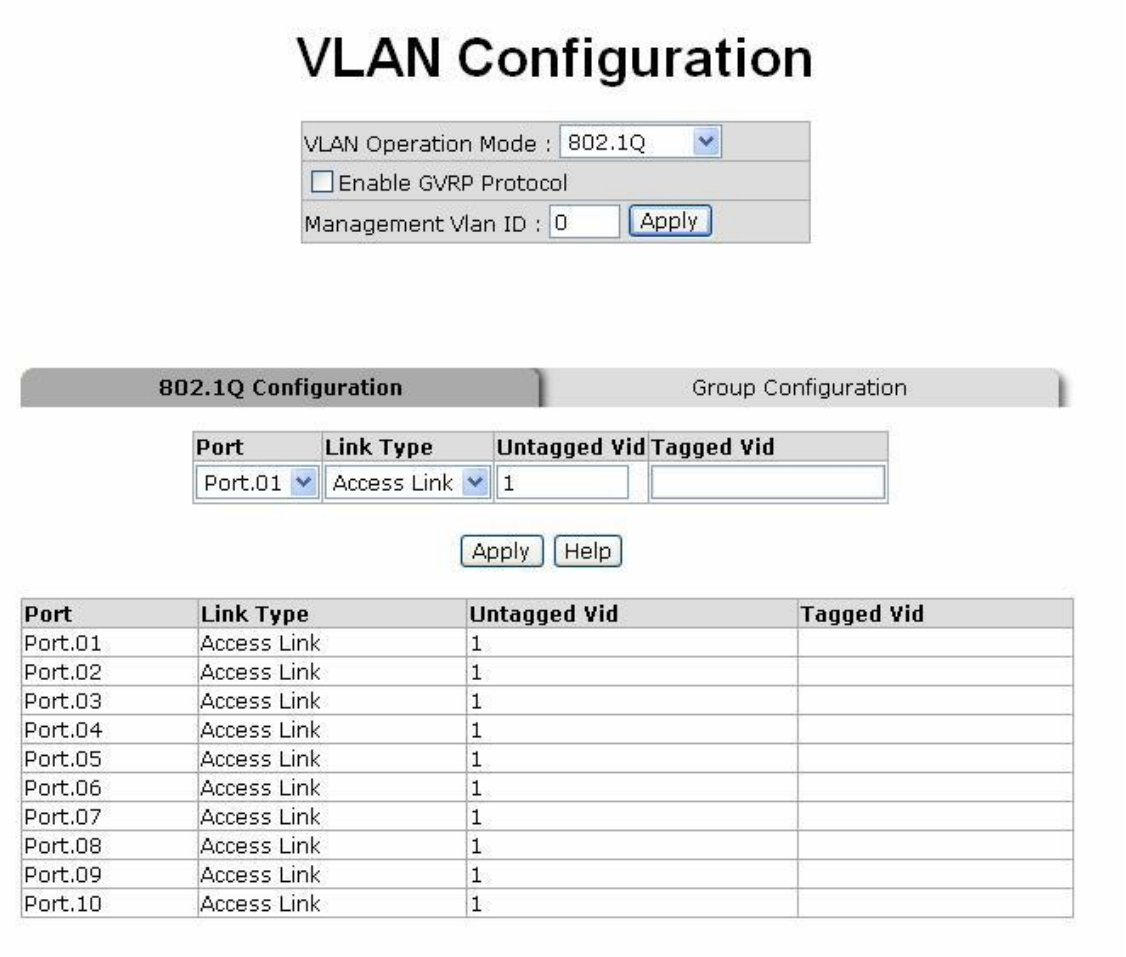
Note	Remember to execute the 'Save Configuration' action, otherwise the new configuration will lose when switch power off.

802.1Q VLAN

Tagged-based VLAN is an IEEE 802.1Q specification standard. Therefore, it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to provide configuring. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 1. The default VLAN can’t be deleted.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



802.1q VLAN interface

802.1Q Configuration

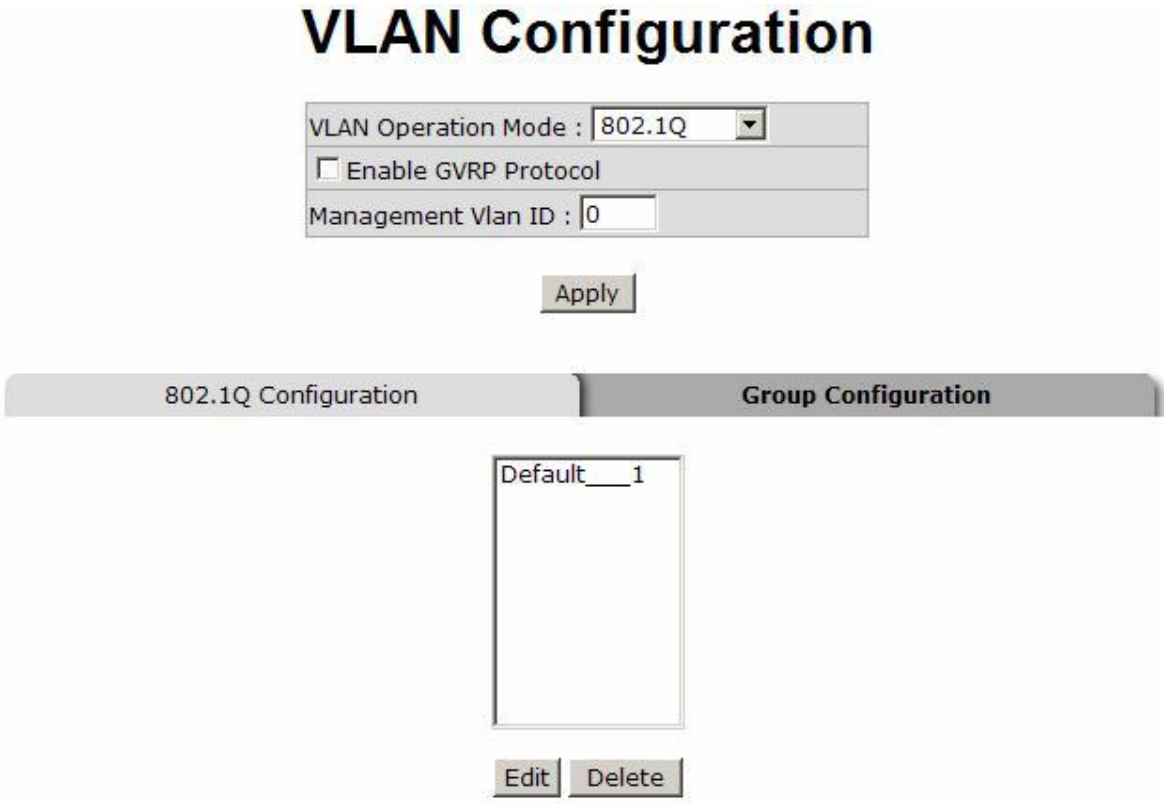
1. Enable GVRP Protocol: Mark the check box to enable GVRP protocol.
2. Select the port that you want to configure.
3. Link Type:
   - ¢ Access Link: Single switch only, allows user to group ports by setting the same VID to those ports.
   - ¢ Trunk Link: The extended application of Access Link. While the ports are set in this type, they can forward the packets with specified tag among the switches which are included in the same VLAN group.
   - ¢ Hybrid Link: Both Access Link and Trunk Link are available.

4. Untagged VID: Assign the untagged frame VID.
5. Tagged VID: Assign the tagged frame VID.
6. Click Apply

Group Configuration

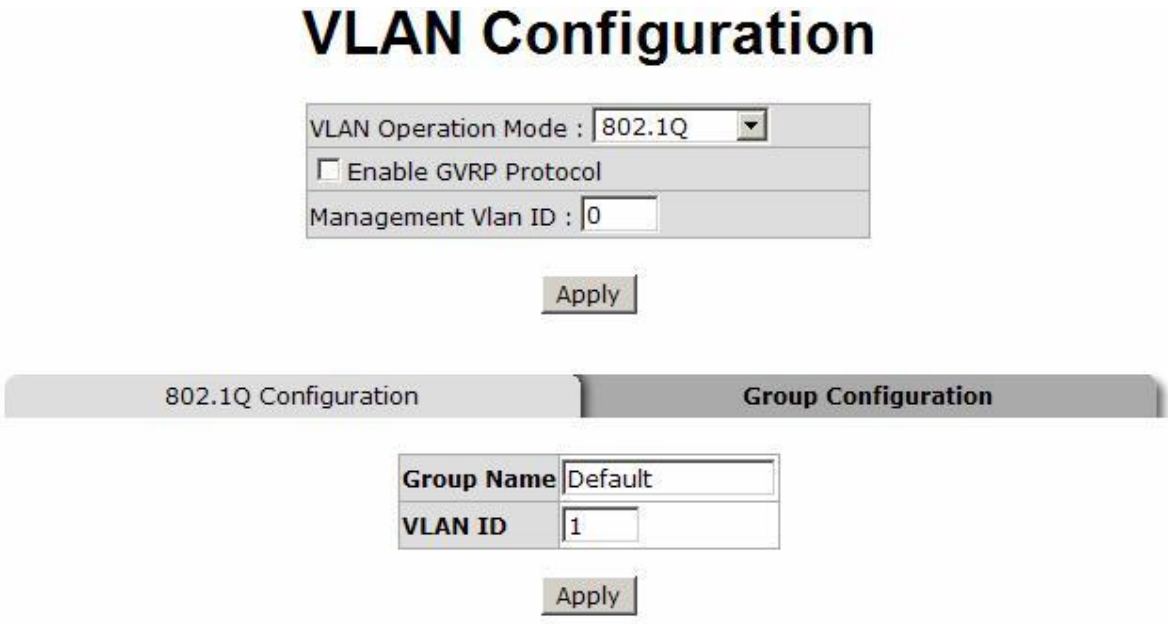
Edit the existing VLAN Group.

1. Select the VLAN group in the table list.
2. Click Apply



Group Configuration interface

3. You can Change the VLAN group name and VLAN ID.
4. Click Apply.



Group Configuration interface

Rapid Spanning Tree

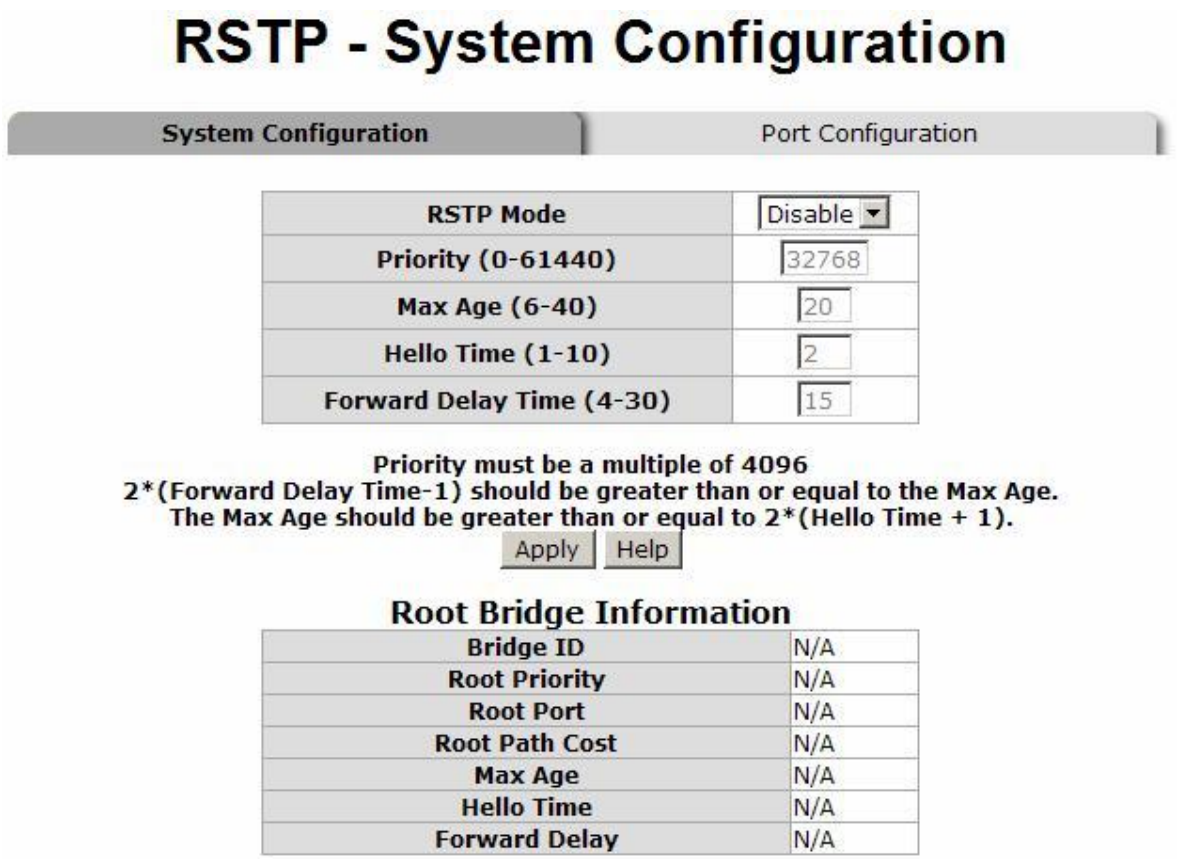
The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will automatically detect the connected device that is running STP or RSTP protocol.

RSTP - System Configuration

- ¢ User can view spanning tree information about the Root Bridge
- ¢ User can modify RSTP state. After modification, click Apply button
  - ‹ RSTP mode: User must enable or disable RSTP function before configuring the related parameters
  - ‹ Priority (0-61440): A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, user must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule

- Max Age (6-40): The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40
- Hello Time (1-10): The time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10
- Forward Delay Time (4-30): The number of seconds a port waits before changing from its Rapid Spanning Tree Protocol learning and listening STP states to the forwarding state. Enter a value between 4 through 30

Note	Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time. 2 x (Forward Delay Time value – 1) > = Max Age value >= 2 x (Hello Time value +1)

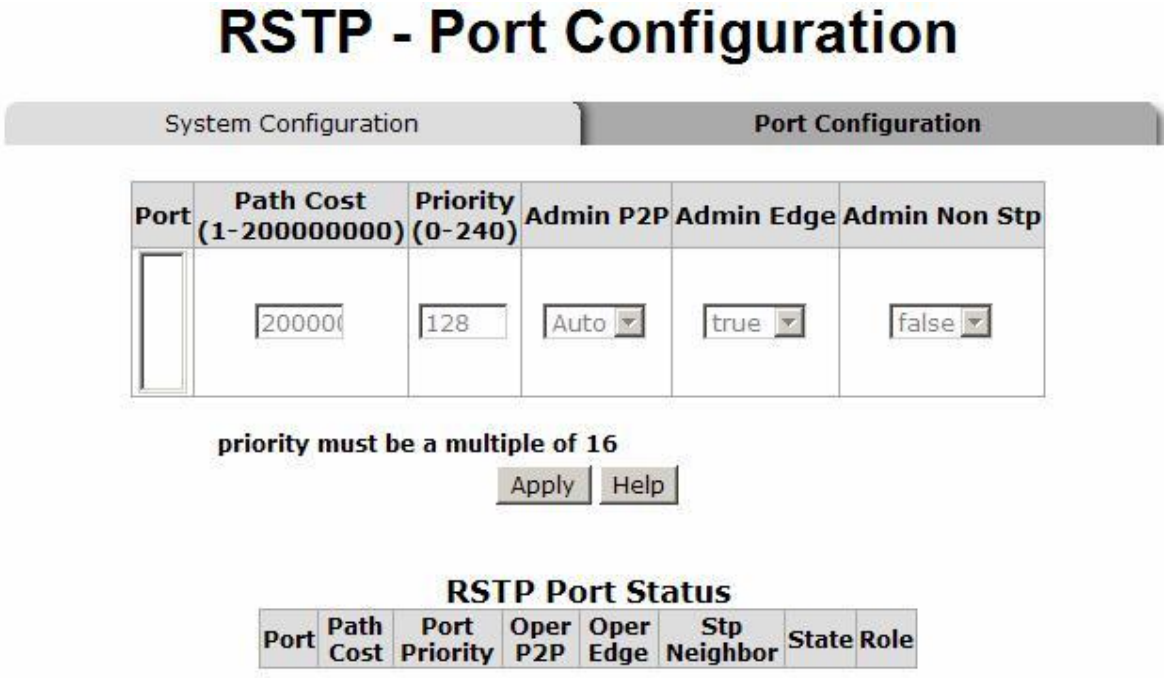


RSTP System Configuration interface

RSTP - Port Configuration

You can configure the path cost and priority of every port.

1. Select the port in Port column.
2. Path Cost: The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
3. Priority: Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16.
4. P2P: Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.
5. Edge: The port directly connected to end stations cannot create bridging loop in the network. To configure the port as an edge port, set the port to “True” status.
6. Non STP: The state of whether the port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation.
7. Click Apply.



RSTP Port Configuration interface

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

System Configuration

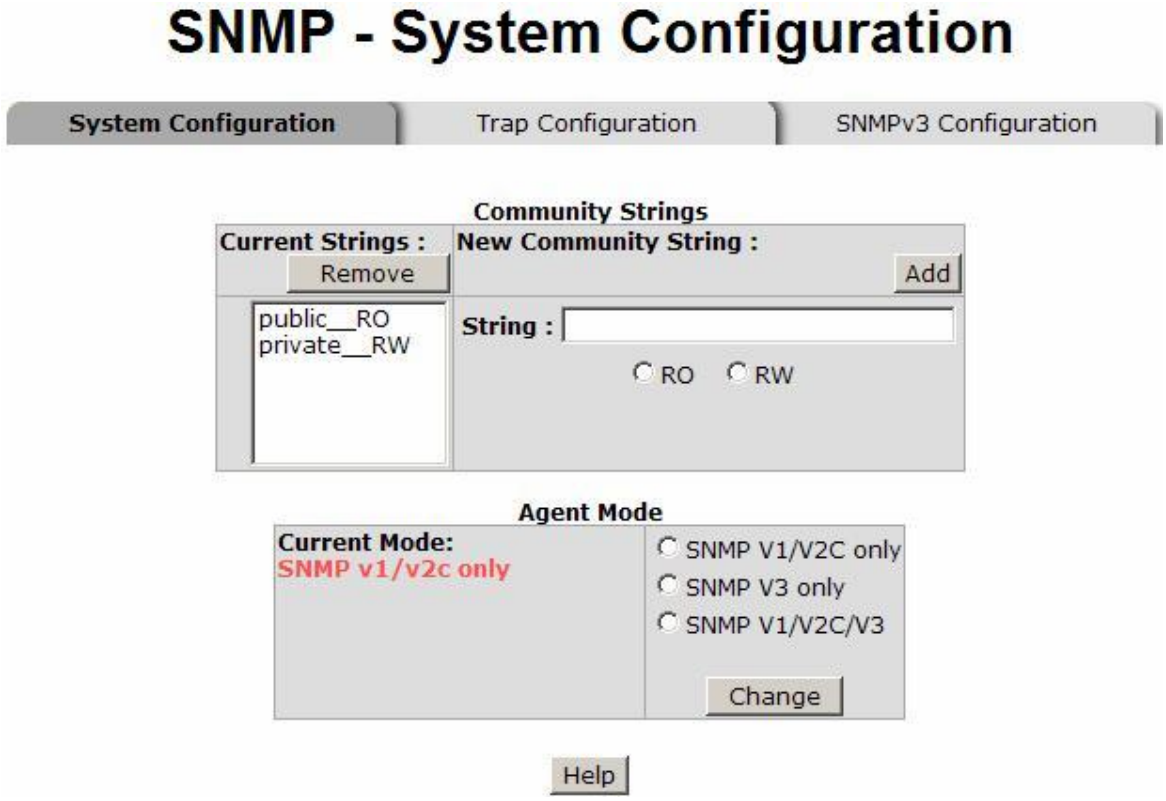
¢ Community Strings

Here you can define new community string set and remove unwanted community string.

1. String: Fill the name of string.
2. RO: Read only. Enables requests accompanied by this string to display MIB-object information.
3. RW: Read & write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

1. Click Add.
2. To remove the community string, select the community string that you have defined and click Remove. You cannot edit the name of the default community strings.

¢ Agent Mode: Select the SNMP version that you want to use it. And then click Change to switch to the selected SNMP version mode.



SNMP System Configuration interface

Trap Configuration

A trap manager is a management station that receives traps and the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager, enter SNMP community strings and selects the SNMP version.

1. IP Address: Enter the IP address of trap manager.
2. Community: Enter the community string.
3. Trap Version: Select the SNMP trap version type – v1 or v2c.
4. Click Add.
5. To remove the community string, select the community string that you have defined and click Remove. You cannot edit the name of the default community string set.

Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

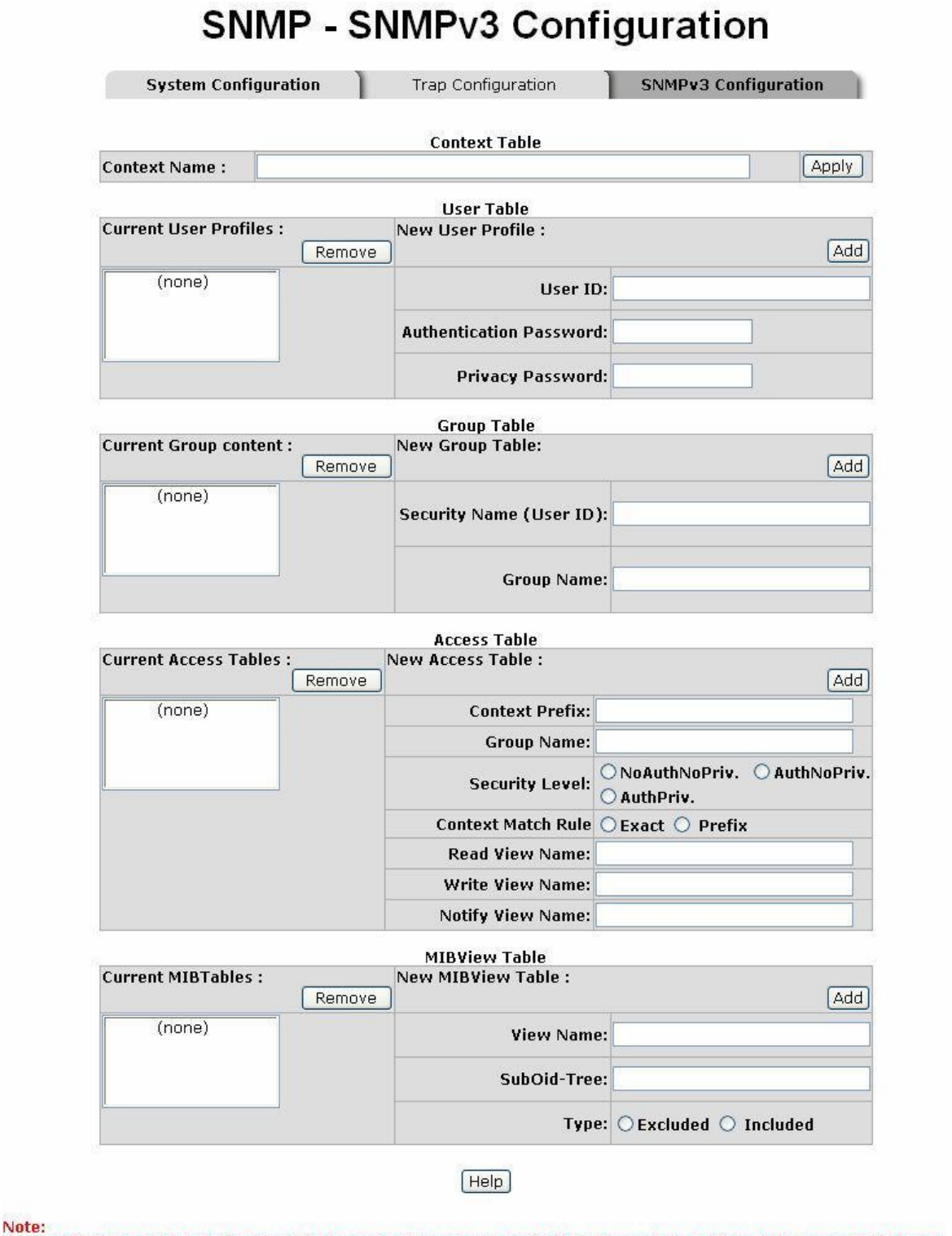
Context Table

Configure SNMP v3 context table. Assign the context name of context table. Click Add to add context name. Click Remove to remove unwanted context name.

User Profile

Configure SNMP v3 user table.

- User ID: Set up the user name.
- Authentication Password: Set up the authentication password.
- Privacy Password: Set up the private password.
- Click Add to add context name.
- Click Remove to remove unwanted context name.



SNMP V3 configuration interface

Group Table

Configure SNMP v3 group table.

- Security Name (User ID): Assign the user name that you have set up in user table.
- Group Name: Set up the group name.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

Access Table

Configure SNMP v3 access table.

- Context Prefix: Set up the context name.
- Group Name: Set up the group.
- Security Level: Set up the access level.
- Context Match Rule: Select the context match rule.
- Read View Name: Set up the read view.
- Write View Name: Set up the write view.
- Notify View Name: Set up the notify view.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

MIBview Table

Configure MIB view table.

- ViewName: Set up the name.
- Sub-Oid Tree: Fill the Sub OID.
- Type: Select the type – exclude or included.

¢ Click Add to add context name.

¢ Click Remove to remove unwanted context name.

QoS Configuration

You can configure QoS policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

¢ Qos Policy: select the QoS policy rule.

‹ Using the 8,4,2,1 weight fair queue scheme: The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example, when the system processes, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.

‹ Use the strict priority scheme: Always higher queue will be process first, except higher queue is empty.

¢ Priority Type: There are 5 priority type selections available. Disable means no priority type is selected.

¢ Port-base: The port priority will follow the Port-base that you have assigned – High, middle, low, or lowest.

‹ COS only: The port priority will only follow the COS priority that you have assigned.

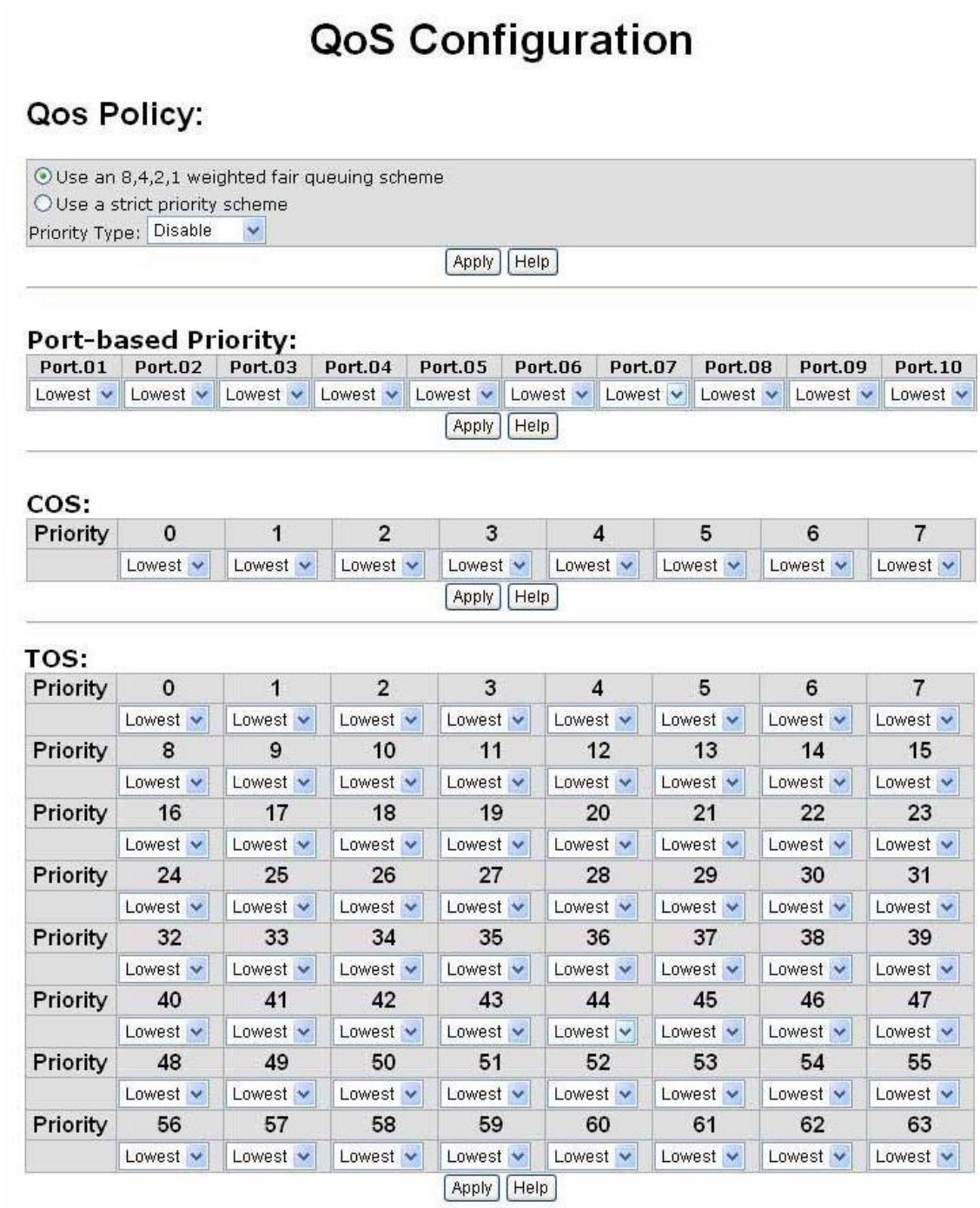
‹ TOS only: The port priority will only follow the TOS priority that you have assigned.

‹ COS first: The port priority will follow the COS priority first, and then other priority rule.

‹ TOS first: the port priority will follow the TOS priority first, and the other priority

rule.

¢ Click Apply.


QoS Configuration
Qos Policy:
Use an 8,4,2,1 weighted fair queuing scheme
Use a strict priority scheme
Priority Type: Disable
Apply Help
Port-based Priority:
Port.01 Port.02 Port.03 Port.04 Port.05 Port.06 Port.07 Port.08 Port.09 Port.10
Lowest
Apply Help
COS:
Priority 0 1 2 3 4 5 6 7
Lowest
Apply Help
TOS:
Priority 0 1 2 3 4 5 6 7
Priority 8 9 10 11 12 13 14 15
Priority 16 17 18 19 20 21 22 23
Priority 24 25 26 27 28 29 30 31
Priority 32 33 34 35 36 37 38 39
Priority 40 41 42 43 44 45 46 47
Priority 48 49 50 51 52 53 54 55
Priority 56 57 58 59 60 61 62 63
Apply Help

QoS Configuration interface

Port Base Priority

Configure per port priority level.

- Port: Each port has 4 priority levels – High, Middle, Low, and Lowest.
- Click Apply.

COS Configuration

Set up the COS priority level.

- COS priority: Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click Apply.

TOS Configuration

Set up the TOS priority.

- TOS priority: The system provides 0~63 TOS priority level. Each level has 4 types of priority – high, middle, low, and lowest. The default value is 'Lowest' priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, user set the TOS level 25 as high, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25 (priority = high), and then the packet priority will have highest priority.
- Click Apply.

IGMP Configuration

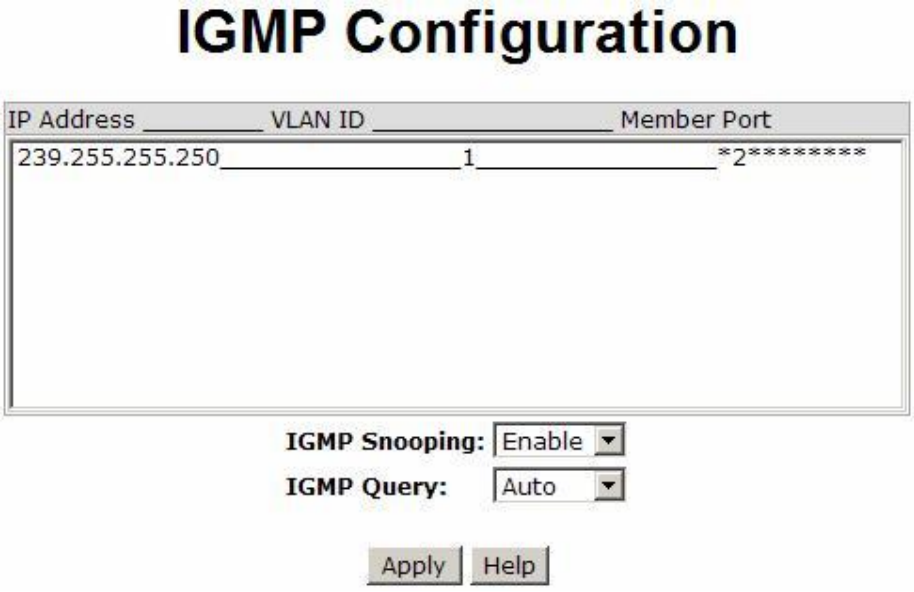
The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts

that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The switch supports IP multicast. You can enable IGMP protocol via setting IGMP configuration page to see the IGMP snooping information. IP multicast addresses are in the range of 224.0.0.0 through 239.255.255.255.

- IGMP Protocol: Enable or disable the IGMP protocol.
- IGMP Query: Select the IGMP query function as Enable or Auto to set the switch as a querier for IGMP version 2 multicast networks.
- Click Apply .



IGMP Configuration interface

X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms not the same.

In the X-Ring topology, every switch should enable X-Ring function and assign two member ports in the ring. Only one switch in the X-Ring group would be set as a master switch that would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port will automatically become a working port to recovery the failure.

The switch supports the function and interface for setting the switch as the ring master or slave mode. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, then software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode will be enabled by the X-Ring configuration interface. Also, user can identify the switch as the ring master from the R.M. LED panel of the LED panel on the switch.

The system also supports the coupling ring that can connect 2 or more X-Ring group for the redundant backup function and dual homing function that prevent connection lose between X-Ring group and upper level/core switch.

¢ Enable X-Ring: Enable the X-Ring function. Mark the check box to enable the X-Ring function.

¢ Enable Ring Master: Mark the check box to enable this machine to be the ring master.

¢ 1st & 2nd Ring Ports: Pull downthe selection menu to assign two ports as the member ports. The 1st Ring Port and 2nd Ring Port are basically assigned to be forwarding ports except for the Ring Master switch. With the Ring Master switch, one of its two Ring Ports is the blocking port and another one is the forwarding port.

Once its forwarding port fails, the system will automatically upgrade its blocking port to be the forwarding port of the Ring Master switch.

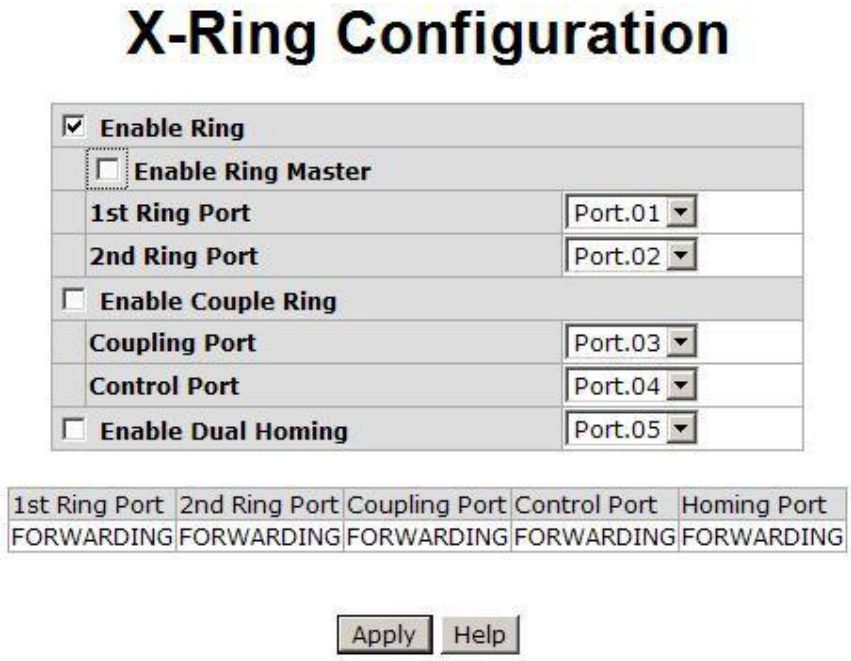
¢ Enable Coupling Ring: Enable the coupling ring function. Mark the check box to enable the coupling ring function.

¢ Coupling port: Assign the member port which is connected to the other ring group.

¢ Control port: When Couple Ring check box is marked, you have to assign the control port to form a couple-ring group between the two X-rings.

¢ Enable Dual Homing: Set up one of the ports on the switch to be the Dual Homing port. For a switch, there is only one Dual Homing port. Dual Homing function only works when the X-Ring function enabled.

¢ And then, click Apply to apply the configuration.



X-ring Interface

Note	When the X-Ring function enable, user must disable the RSTP. The X-Ring function and RSTP function cannot exist in a switch at the same time. Remember to execute the 'Save Configuration' action, otherwise the new configuration will lose when switch power off.

¢ Security

In this section, you can configure 802.1x and MAC address table.

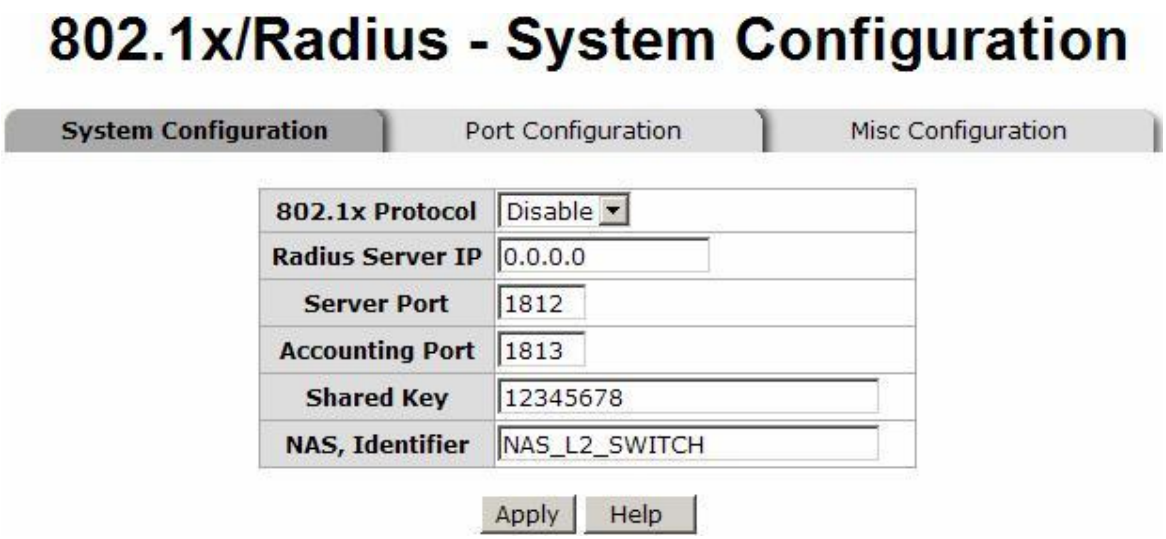
802.1X/Radius Configuration

802.1x is an IEEE authentication specification prevents the client from connecting to a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server.

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

1. IEEE 802.1x Protocol: Enable or disable 802.1x protocol.
2. Radius Server IP: Set the Radius Server IP address.
3. Server Port: Set the UDP destination port for authentication requests to the specified Radius Server.
4. Accounting Port: Set the UDP destination port for accounting requests to the specified Radius Server.
5. Shared Key: Set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
6. NAS, Identifier: Set the identifier for the radius client.
7. Click Apply.



802.1x System Configuration interface

802.1x Per Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Hit “Space” key to change the state value.

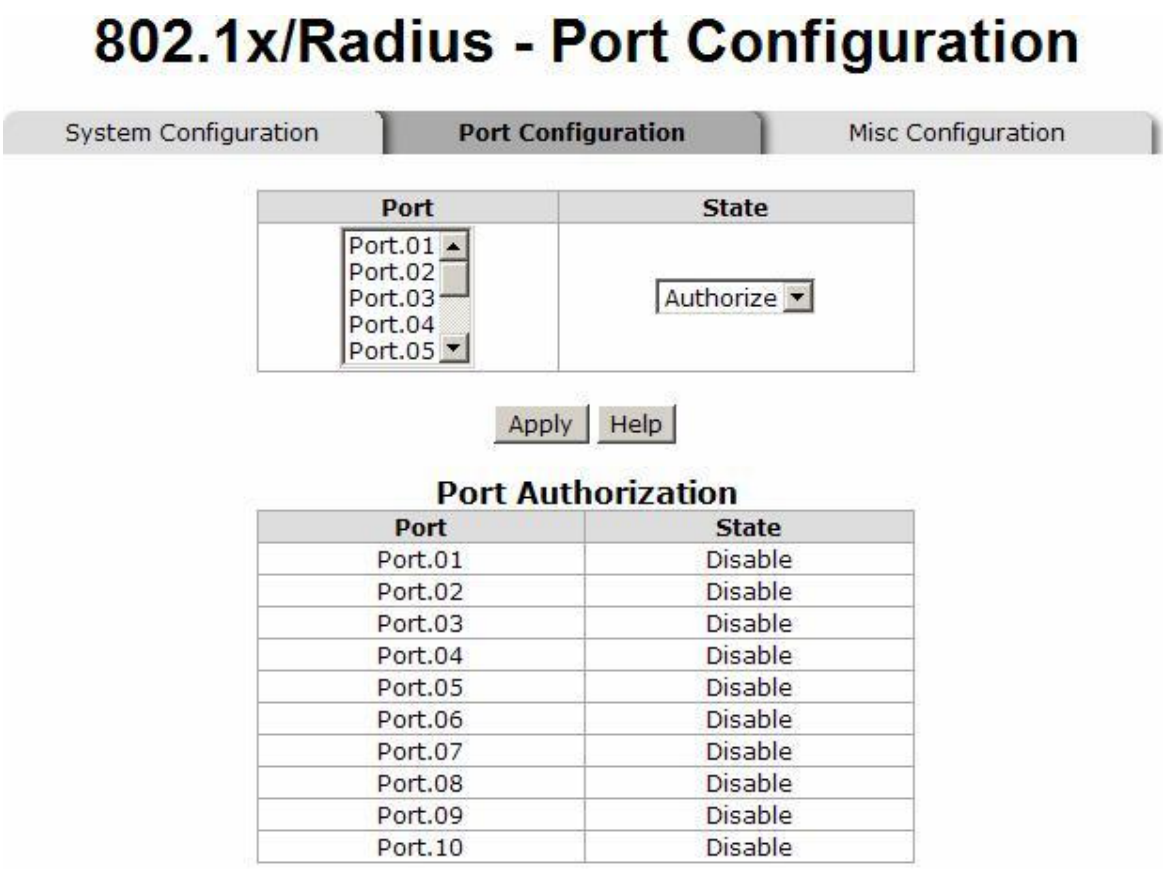
¢ Reject: The specified port is required to be held in the unauthorized state.

¢ Accept: The specified port is required to be held in the Authorized state.

¢ Authorized: The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the supplicant and the authentication server.

¢ Disable: When disabled, the specified port works without meeting 802.1x protocol.

¢ Click Apply.

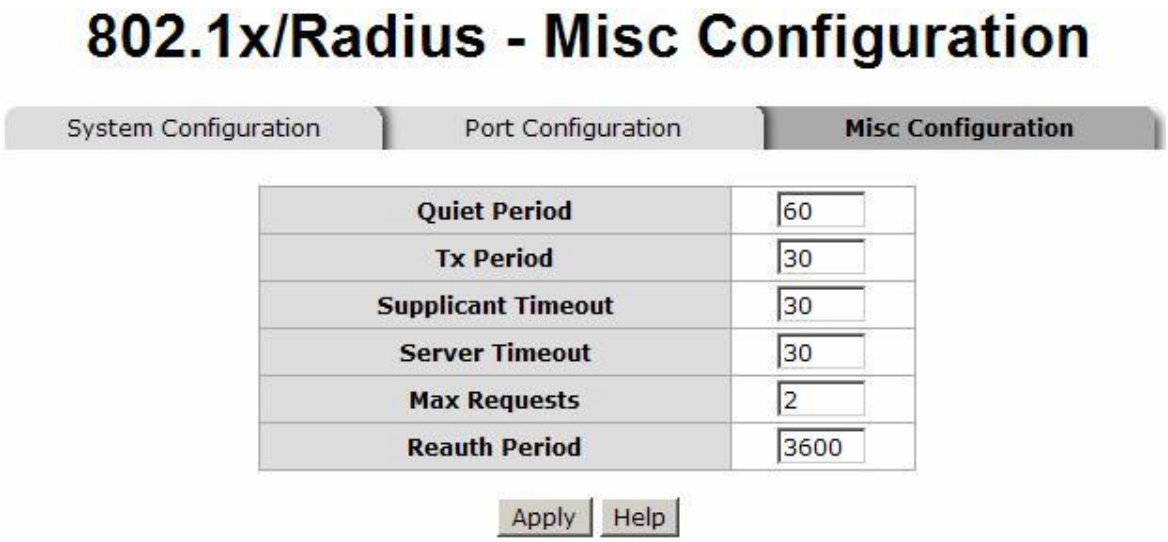


802.1x Per Port Setting interface

Misc Configuration

1. Quiet Period: Set the period which the port doesn't try to acquire a supplicant.
2. TX Period: Set the period the port waits for retransmit next EAPOL PDU during an authentication session.
3. Supplicant Timeout: Set the period of time the switch waits for a supplicant response to an EAP request.
4. Server Timeout: Set the period of time the switch waits for a server response to an authentication request.
5. Max Requests: Set the number of authentication that must time-out before authentication fails and the authentication session ends.
6. Reauth period: Set the period of time which clients connected must be re-authenticated.

7. Click Apply.



802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure the port security.

Static MAC Address

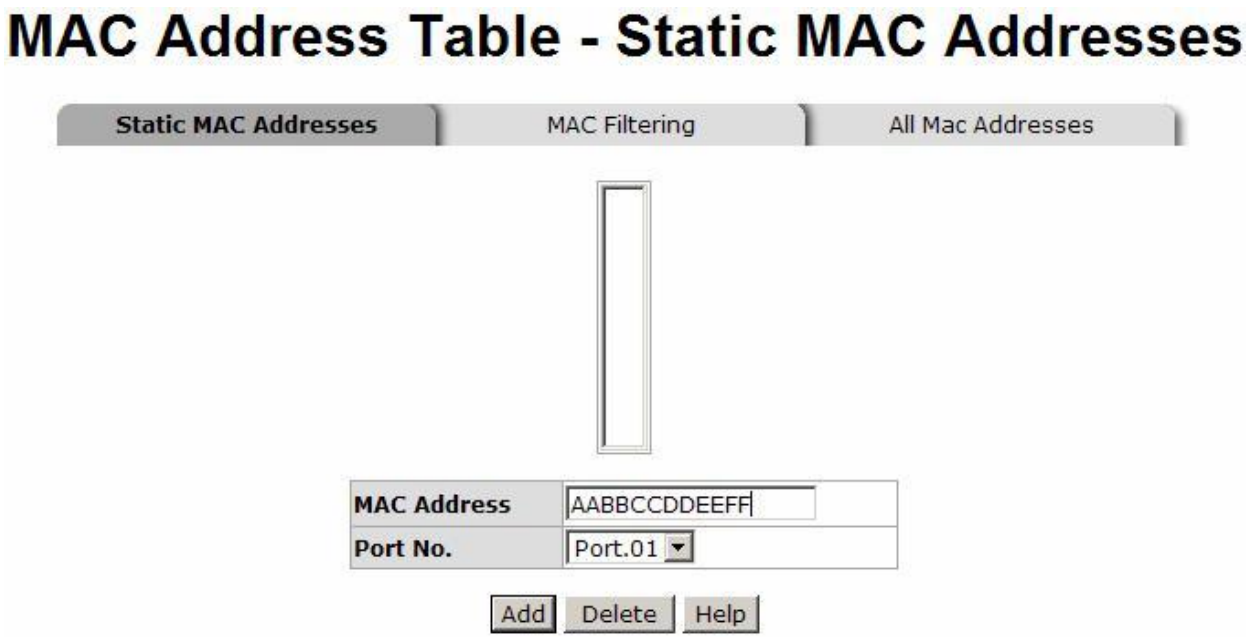
You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add/ modify/delete a static MAC address.

¢ Add the Static MAC Address

You can add static MAC address in the switch MAC table.

1. MAC Address: Enter the MAC address of the port that should permanently forward traffic regardless of the device network activity.
2. Port No.: Pull down the selection menu to select the port number.

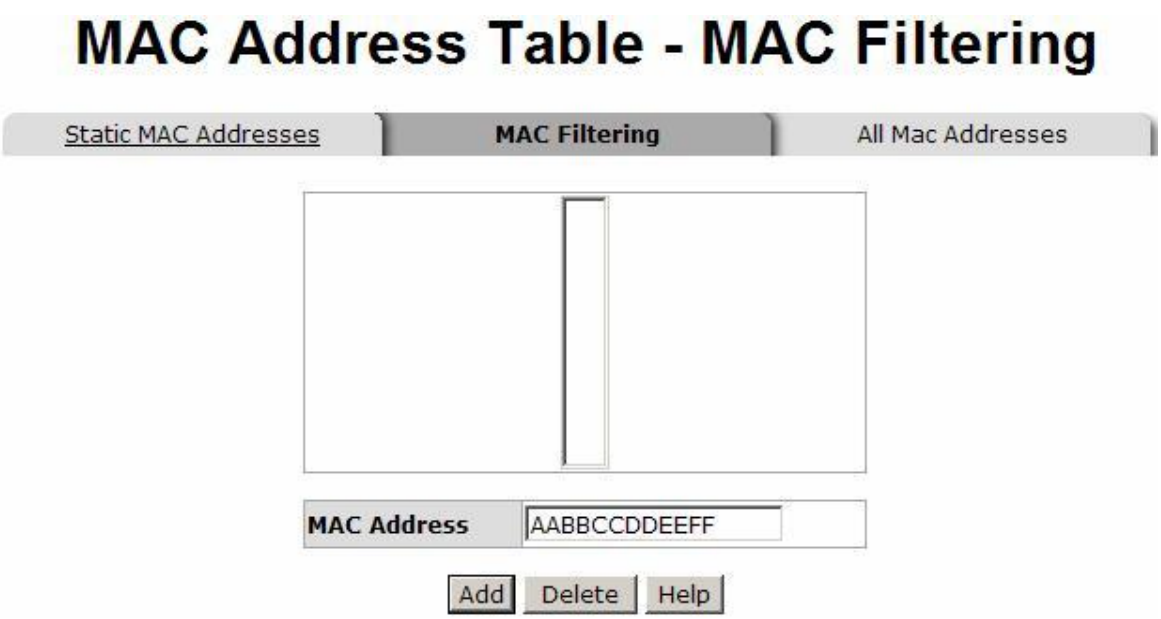
3. Click Add .
4. If you want to delete the MAC address from filtering table, select the MAC address and click Delete .



Static MAC Addresses interface

MAC Filtering

By filtering MAC address, the switch can easily filter pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address.



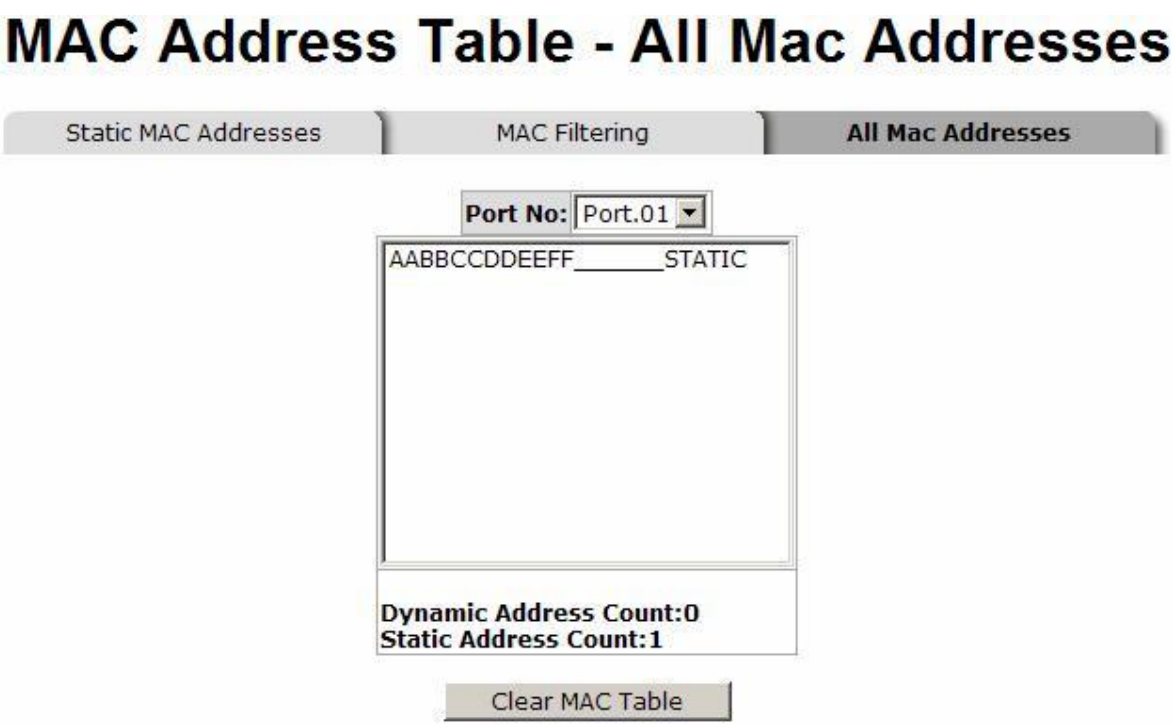
MAC Filtering interface

1. MAC Address: Enter the MAC address that you want to filter.
2. Click Add.
3. If you want to delete the MAC address from filtering table, select the MAC address and click Delete.

All MAC Addresses

You can view the port information of the connected device's MAC address and related devices' MAC address.

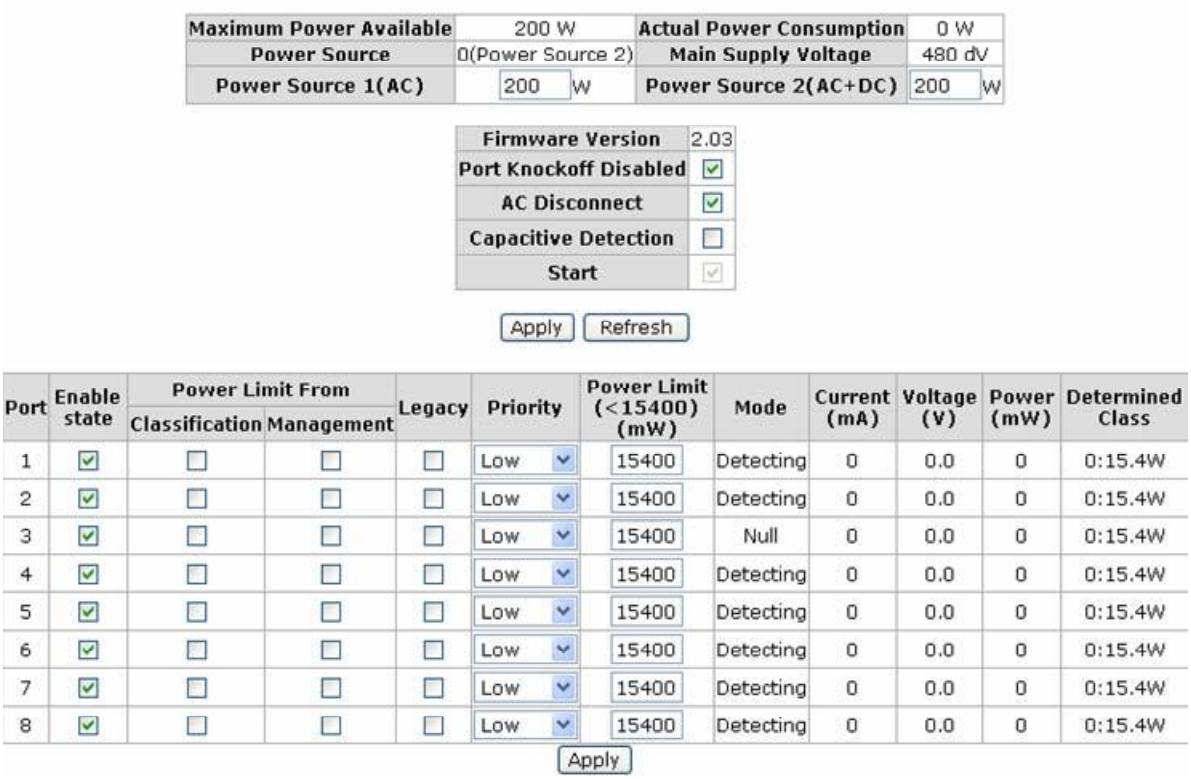
1. Select the port.
2. The selected port of dynamic & static MAC address information will be displayed here.
3. Click Clear MAC Table to clear the current port static MAC address information on screen.



All MAC Address interface

Power over Ethernet

This segment shows the Power over Ethernet function.



Maximum Power Available	200 W	Actual Power Consumption	0 W
Power Source	0(Power Source 2)	Main Supply Voltage	480 dV
Power Source 1(AC)	200 W	Power Source 2(AC+DC)	200 W

Firmware Version	2.03
Port Knockoff Disabled	☑
AC Disconnect	☑
Capacitive Detection	☐
Start	☑

Apply Refresh

Port	Enable state	Power Limit From		Legacy	Priority	Power Limit (<15400) (mW)	Mode	Current (mA)	Voltage (V)	Power (mW)	Determined Class
		Classification	Management								
1	☑	☐	☐	☐	Low	15400	Detecting	0	0.0	0	0:15.4W
2	☑	☐	☐	☐	Low	15400	Detecting	0	0.0	0	0:15.4W
3	☑	☐	☐	☐	Low	15400	Null	0	0.0	0	0:15.4W
4	☑	☐	☐	☐	Low	15400	Detecting	0	0.0	0	0:15.4W
5	☑	☐	☐	☐	Low	15400	Detecting	0	0.0	0	0:15.4W
6	☑	☐	☐	☐	Low	15400	Detecting	0	0.0	0	0:15.4W
7	☑	☐	☐	☐	Low	15400	Detecting	0	0.0	0	0:15.4W
8	☑	☐	☐	☐	Low	15400	Detecting	0	0.0	0	0:15.4W

Apply

PoE Status

- Maximum Power Available: Displays the maximum power supply in Watt.
- Actual Power Consumption: This column shows the real-time total power consumption.
- Power Source: This column shows the power source which is supplying.
- Power Source 1 (AC): This column shows the supplying power value of power source 1.
- Power Source 2 (AC+DC): This column shows the supplying power of power source 2.
- Firmware Version: This column shows the PoE chip's firmware version.
- AC Disconnect: Mark this check box to monitor the AC impedance on the port terminals and removes power when the impedance rises above a certain value, for a

certain period (for details, see the IEEE 802.3af specification).

- Capacitive Detection: If the port and capacitive detection are enabled, the capacitances state reads in the voltage result from the constant current. This is the subtracted from the pre-capacitance voltage to get a charge rate. If this charge rate is within the window of the PD signatures, the device is considered to be discovered.
- And then, click Apply to carry into effect.
- Port: The index of PoE ports.
- Enable State: Check it to enable the PoE function to the port.
- Power Limit From: Check it to decide the power limit method.
  - Classification: When this check box is marked, the system will limit the power supply to the powered device in accordance with the related class.
- Legacy: Check it to support the legacy power devices.
- Priority: Pull down the selection menu item to choose the priority of power supplying.
- Port Limit (<15400) mW: User can key in the power limit value which is under 15.4 Watts.
- Mode: Displays the operating mode of the port.
- Current (mA): Displays the operating current of the port.
- Voltage (V): Displays the operating voltage of the port.
- Power (mW): Displays the power consumption of the port.
- Determined Class: Displays the PD's class.
- And then, click Apply to carry into effect.

Factory Default

Reset switch to default configuration. Click Reset to reset all configurations to the default value.

Factory Default interface

Save Configuration

Save all configurations that you have made in the system. To ensure the all configuration will be saved. Click Save to save the all configuration to the flash memory.

Save Configuration interface

System Reboot

Reboot the switch in software reset. Click Reboot to reboot the system.

System Reboot interface

Troubleshooting

This section is intended to help solve the most common problems on the PoE Injector Managed Switch.

Incorrect connections

The switch port can automatically detect straight or crossover cable when you link switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps port use 2-pairs twisted cable and Gigabit 1000T port use 4 pairs twisted cable. If the RJ-45 connector is not correctly pinned on right position then the link will fail. For fiber connection, please notice that fiber cable mode and fiber module should be match.

- Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.

- Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5-cable tester is a recommended tool for every 100Base-T network installation.

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100 Ω Category 3, 4 or 5 cable for 10Mbps connections, Ω00 Category 5 cable for 100Mbps connections, or 100Ω Category 5e/above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

¢ Improper Network Topologies

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

Diagnosing LED Indicators

The switch can be easily monitored through panel indicators, which describes common problems user may encounter and where user can find possible solutions, to assist in identifying problems.

If the power indicator does not light on when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the Switch powers off after running for a while; check for loose power connections, power losses, or surges at power outlet. If the problem still cannot be resolved, please contact the local dealer for assistance.

Technical Specification

This section provides the specifications of 8 10/100TX + 2 Gigabit copper/ Mini-GBIC Combo with 8 PoE Injectors Managed Switch.

.

Standard	IEEE802.3 10BASE-T Ethernet IEEE802.3u 100BASE-TX IEEE802.3ab 1000Base-T IEEE802.3z Gigabit fiber IEEE802.3x Flow control and Back pressure IEEE802.3ad Port trunk with LACP IEEE802.3af Power over Ethernet Cisco Legacy PD IEEE802.1d Spanning Tree IEEE802.1w Rapid spanning tree IEEE802.1p Class of service IEEE802.1Q VLAN Tag IEEE 802.1x user authentication(Radius) IEEE802.1ab LLDP** (for 8 10/100TX + 2 Gigabit copper/Mini-GBIC Combo with 8 PoE Injectors Managed Switch)
LED Indicators	System Power: (Green) 10/100TX Port: Link/Activity (Green), 100Mbps (Green) Gigabit copper port: 1000Mbps (Green), Link/Activity (Green) Mini-GBIC: Link/Activity (Green) PoE: FWD (Green)

	Full-duplex/Collision ([Orange], 8 10/100TX + 1 10/100/1000T/100/1000 SFP Combo with 4 PoE Injectors Managed Switch)
Connector	100Base-T: RJ-45 with auto MDI/MDI-X Port 1~8 (8 PoE Injectors model) support POE injecting function 1000Base-T:RJ-45 with auto MDI/MDI-X Gigabit fiber: Mini-GBIC socket 100M fiber: Mini-GBIC socket
Switch architecture	Store and forward switch architecture System throughput up to 8.3Mpps
Back-plane	3.6Gbps (4 PoE Injectors model) 5.6Gbps (8 PoE Injectors model)
MAC address	8K MAC address table with Auto learning function
Flash ROM	4Mbytes
DRAM	32Mbytes
Packet Buffer	1Mbits for packet buffer
Power Supply	100~240V_{AC} DC 48V (8 PoE Injectors model)
Power Consumption	79Watts (4 PoE Injectors model)

	135Watts (8 PoE Injectors model)
Ventilation	1 fan
Operating Temperature	0℃~45℃, 5%~95%RH
Storage environment	-40℃ -70℃
Dimensions	270mm(W) x 210mm(D) x 4mm(H)
EMI	FCC Class A CE
Safety	UL, cUL, CE/EN60950-1

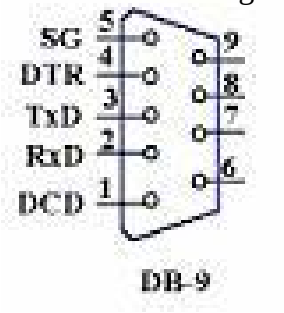
** optional

Appendix

Console Port Pin Assignments

The DB-9 serial port on the switch is used to connect to the switch for out-of-band

console configuration. The console—command line interface can be accessed from a terminal or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.



DB-9 Console Port Pin Numbers

¢ DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #
BB	104	RxD (Received Data)	2	2
BA	103	TxD (Transmitted Data)	3	3
AB	102	SGND (Signal Ground)	5	5

¢ Console Port to 9-Pin DTE Port on PC

Switch's 9-Pin Serial Port	CCITT Signal PC's 9-Pin	DTE Port
2 RXD	<---------RXD ----------	3 TxD
3 TXD	----------TXD --------=>	2 RxD
5 SGND	----------SGND ----------	5 SGND

100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and

pins 3 and 6 for receiving data; pins 4, 5, 7 and 8 are used for power supplying.

RJ-45 Pin Assignment of non-802.3af standard PD with Midspan/Endspan POE HUB/SWITCH

¢ Pin out of Cisco non-802.3af standard PD

Pin	Signal
1	RX+
2	RX-
3	TX+
4	VCC -
5	VCC -
6	TX-
7	VCC +
8	VCC +

¢ Pin out of POE Midspan Hub/Switch

Pin	Signal / Name
1	RX+
2	RX-
3	TX+
4	VCC+
5	VCC+
6	TX-
7	VCC-
8	VCC-

¢ Pin out of POE Endspan Hub/Switch

Pin	Signal / Name
1	TX+/VCC+
2	TX-/VCC+
3	TX+/VCC-
4	
5	
6	TX-/VCC-
7	
8	

Note ‘+’ and ‘-‘ signs represent the polarity of the wires that make up each wire pair.
Before you powered PD, please check the RJ-45 connector pin assignment follow IEEE802.3af standard, otherwise you may need change one of the RJ-45 connector pin assignment, which attached with the UTP cable.

All ports on this switch support automatic MDI/MDI-X operation, you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3 and 6, at one end of the cable,

are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

Pin MDI-X	Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)